TESIS DOCTORAL

UNAI ABERASTURI GORRIÑO

LOS PRINCIPIOS DE LA PROTECCIÓN DE DATOS APLICADOS EN LA SANIDAD

Presentada para la obtención del grado de Doctor en Derecho bajo la dirección del Doctor D. IÑAKI LASAGABASTER HERRARTE, Catedrático de Derecho Administrativo, en el Departamento de Derecho Administrativo, Constitucional y Filosofía del Derecho de la Universidad del País Vasco-Euskal Herriko Unibertsitatea.

Bilbao 2011

ISBN: 978-84-9860-581-5

ÍNDICE.

CAPÍTULO 2. CUESTIONES PREVIAS AL ANÁLISIS DE LOS PRINCIPIOS BÁSICOS QUE RIGEN LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SANITARIOS.

CAPÍTULO 6. LOS DERECHOS DE LOS PACIENTES CON RESPECTO A LOS DATOS SANITARIOS QUE LES CONCIERNEN.

ABREVIATURAS

AA	*Actualidad Administrativa*
AAP	Auto de la Audiencia Provincial
AC	*Actualidad Civil*
AEPD	Agencia Española de Protección de Datos
AJCA	Auto del Juzgado de lo Contencioso Administrativo
AIA	*Actualidad Informática Aranzadi*
AJA	*Actualidad Jurídica Aranzadi*
AJR	*Anuario Jurídico de la Rioja*
AP	*Actualidad Penal*
APD	Agencia de Protección de Datos
APDCat	Agencia de Protección de Datos de Cataluña
APDCM	Agencia de Protección de Datos de la Comunidad de Madrid
ATC	Auto del Tribunal Constitucional
AVPD	Agencia Vasca de Protección de Datos
BJC	*Boletín de Jurisprudencia Constitucional*
BOCG	Boletín Oficial de las Cortes Generales
BOE	Boletín Oficial del Estado
BOPV	Boletín Oficial del País Vasco
CAPV	Comunidad Autónoma del País Vasco
CC	Código Civil
CCAA	Comunidades Autónomas
CE	Constitución Española de 1978
CEC	Centro de Estudios Constitucionales
CEDH	Convenio Europeo de Derechos Humanos
CEPC	Centro de Estudios Políticos y Constitucionales
CERA	Centro de Estudios Ramón Areces
CES	Consejo Económico Social
CGPJ	Consejo General del Poder Judicial
CP	Código Penal
DA	Disposición Adicional
DAD	*Documentación Administrativa*
DO	Diario Oficial
DS	*Derecho y Salud*
EDJ	*Estudios de Derecho Judicial*
EFTA	*European Free Trade Asociation*

FJ	Fundamento Jurídico
GAPP	*Gestión y Análisis de Políticas Públicas*
INAP	Instituto Nacional de Administración Pública
IVAP-HAEE	Instituto Vasco de Administración Pública-Herri Arduralaritzaren Euskal Erakundea
IyD	*Informática y Derecho*
IyS	*Informática y Salud*
LAE	Ley 11/2007, 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos
LBAP	Ley 41/2002, 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica
LBRL	Ley 7/1985, 2 de abril, reguladora de las Bases del Régimen Local
LEC	Ley 1/2000, 7 de enero, de Enjuiciamiento Civil
LECrim	Ley de Enjuiciamiento Criminal (RD 14 de septiembre de 19882)
LGS	Ley 14/1986, 25 de abril, General de Sanidad
LJCA	Ley 29/1998, 13 de julio, reguladora de la Jurisdicción Contencioso Administrativa
LO	Ley Orgánica
LOPD	Ley Orgánica 15/1999, 13 de diciembre, de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica, 6/1985, 1 de julio, del Poder Judicial
LORTAD	Ley Orgánica 5/1992, 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
LPAC	Ley 30/1992, 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común
OCDE	Organización para la Cooperación y el Desarrollo Económico
RAAP	*Revista Andaluza de Administración Pública.*
RAE	Real Academia Española
RAP	*Revista de Administración Pública*
RCDP	*Revista Catalana de Dret Public*
RD	Real Decreto
RDCE	*Revista de Derecho Constitucional Europeo*
RDGH	*Revista de Derecho y Genoma Humano*
RDL	Real Decreto Legislativo
RDLOPD	Reglamento de Desarrollo de la LOPD
RDP	*Revista de Derecho Político*
REDA	*Revista Española de Derecho Administrativo*
REDC	*Revista Española de Derecho Constitucional*
REDI	*Revista Electrónica de Derecho Informático*

REP	*Revista de Estudios Políticos*
REPD	*Revista Española de Protección de Datos*
RFDUC	*Revista de la Facultad de Derecho de la Universidad Complutense*
RFDUG	*Revista de la Facultad de Derecho de la Universidad de Granada*
RGDA	*Revista General de Derecho Administrativo*
RGDP	*Revista General de Derecho Penal*
RJCyL	*Revista Jurídica de Castilla y León*
RPJ	*Revista del Poder Judicial*
RVAP	*Revista Vasca de Administración Pública*
SAN	Sentencia de la Audiencia Nacional
SAP	Sentencia de la Audiencia Provincial
STC	Sentencia del Tribunal Constitucional
STEDH	Sentencia del Tribunal Europeo de Derechos Humanos
STS	Sentencia del Tribunal Supremo
STSJ	Sentencia del Tribunal Superior de Justicia
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea
TC	Tribunal Constitucional
TCE	Tratado Constitutivo de la Comunidad Europea
TEDH	Tribunal Europeo de Derechos Humanos
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea
VVAA	Varios Autores

INTRODUCCIÓN.

Es una idea repetida desde los más diversos foros, que la incorporación de las Tecnologías de la Información y la Comunicación (TIC) en prácticamente todos los ámbitos de la vida se ha acelerado en los últimos veinte años, y que la socialización de las nuevas tecnologías, sobre todo de Internet, y la generalización de su uso ha supuesto un cambio radical en la forma que tienen las personas de relacionarse, de informarse, de disfrutar del ocio, de hacer negocios, de realizar gestiones con las administraciones, etc. Esta transformación acelerada de la sociedad ha planteado múltiples cuestiones que poco a poco han ido teniendo respuesta en la doctrina.

El desarrollo de la Sociedad de la Información y sus efectos es una cuestión que ha sido debatida reiteradamente desde hace tiempo, sin embargo, en los últimos años los estudios sobre las diferentes interrogantes que plantea este fenómeno se han multiplicado. Esto se debe a que las TIC cada vez cuentan con mayor protagonismo en la vida de las personas. Por un lado, constituyen un sector con una creciente relevancia en las economías de todo el mundo. Por otro, los medios de comunicación cada vez otorgan más espacio a comentar aspectos vinculados a estas herramientas. Por último, el interés de la ciudadanía por las nuevas tecnologías es también mayor. No sólo como consumidores interesados en actualizar y renovar sus *tools*, sino también como usuarios preocupados con los efectos de su empleo, los ciudadanos se perfilan como agentes cada vez más implicados en el desarrollo de la Sociedad de la Información. Hay que tomar en consideración, además, que la sociedad sigue transformándose a gran ritmo, generando nuevos problemas que han de ser analizados o exigiendo la revisión de otros que ya se habían planteado.

El especial interés que suscita lo relacionado con las nuevas tecnologías ha tenido reflejo en la gran cantidad de trabajos que se han dedicado a investigar los múltiples efectos que conlleva la consolidación de la Sociedad de la Información. Estos estudios se han realizado desde las más diversas disciplinas o perspectivas: económica, política, cultural, social, etc. Lo que aquí interesa es, precisamente, centrarse en una de estas perspectivas, como es la que vincula las nuevas tecnologías con los derechos humanos y más concretamente con el derecho a la autodeterminación informativa o a la protección de datos.

Hay que tener en cuenta que uno de los puntos de debate más conflictivos que plantean las TIC se sitúa en cómo afecta su uso a los derechos humanos. Son varios los derechos que pueden verse implicados cuando se emplean las nuevas tecnologías en el ejercicio de cualquier actividad. Desde derechos clásicos con firme arraigo en los ordenamientos de gran parte del globo, como el derecho a la intimidad, el honor, la imagen o las libertades de expresión e información, hasta derechos de nueva creación o que necesitan ser reconsiderados, como el derecho a la interconexión, a la protección de datos, a la propiedad intelectual, a la identidad, al olvido etc., los bienes jurídicos que pueden entrar en juego cuando se utilizan las TIC son pues múltiples.

Entre las distintas líneas de investigación dedicadas a analizar la relación entre las nuevas tecnologías y los derechos humanos, una de las cuestiones más debatidas ha sido el efecto que tiene el uso de las primeras en el derecho a la protección de datos de carácter personal o

derecho a la autodeterminación informativa. Hay que tener en cuenta que el valor principal de las TIC lo constituye la creación de un nuevo entorno, el ciberespacio, donde las barreras espaciales y temporales prácticamente desaparecen y se configura una nueva forma de manipular la información con pocos límites. Las posibilidades que articulan las nuevas tecnologías a la hora de tratar datos de carácter personal hacen que la salvaguarda del citado derecho se erija en constante objeto de análisis cuando se estudia la relación nuevas tecnologías-derechos humanos. A diferencia de lo que ha ocurrido con determinados debates que han tenido una repercusión social puntual, caso, por ejemplo, de la defensa de los derechos de propiedad intelectual ante el uso de plataformas para la descarga de contenidos digitales o de la protección de las personas ante el empleo por empresas privadas de mecanismos de captación de imágenes que capturan también datos de redes *wifi* particulares, la discusión en torno a la necesidad de proteger los datos de carácter personal ha supuesto un reto de primer orden que se ha mantenido a lo largo de todo el proceso de consolidación de la tan referida Sociedad de la Información. Prueba de ello es que desde la aprobación de las primeras normas dirigidas a proteger los datos de carácter personal en la década de los 70 hasta el día de hoy, la protección del derecho a la autodeterminación informativa ha sido una preocupación prioritaria para los juristas.

El interés por el estudio de esta materia sigue plenamente vigente. Esta circunstancia viene justificada debido a que el afán por la protección de este derecho ha aumentado en los últimos años. Por un lado, desde un punto de vista social, el *scoring*, el *phising*, el *data mining*, la pérdida o alteración de datos, etc. constituyen en la actualidad realidades cercanas y conocidas, y la ciudadanía cada vez es más consciente de la importancia de controlar lo que sucede con la información que le concierne. Este hecho es fácilmente constatable si se atiende al incremento que han sufrido las consultas y denuncias realizadas por los ciudadanos en las distintas agencias de protección de datos, las resoluciones judiciales dictadas a este respecto, o las noticias publicadas por los medios vinculadas a esta materia, como la aparición de historias clínicas en la basura o la necesidad de garantizar la seguridad en las redes sociales. Por otro, desde una perspectiva jurídica, la actividad del legislador ha sido prolija a la hora de regular la materia de protección de datos. En este sentido en los últimos veinte años se han aprobado en el ámbito estatal dos Leyes orgánicas y diferentes reglamentos que regulan específicamente la protección de datos de carácter personal, además de distintas normas que en ámbitos sectoriales se refieren también, aunque sea tangencialmente, a esta cuestión. Lo mismo ha ocurrido en la esfera internacional, donde tanto en el ámbito de la UE como del Consejo de Europa se han aprobado múltiples normas y adoptado sentencias que se refieren a esta materia.

Nadie duda de que el derecho a la autodeterminación informativa cuenta hoy día con una sólida base jurídica, consolidándose dentro del catálogo de los derechos fundamentales, y una creciente relevancia social. No es de extrañar, por lo tanto, que sean numerosos los trabajos doctrinales publicados en el ámbito estatal que analizan el derecho a la protección de datos desde los más diversos puntos de vista. Hay que considerar que la protección de datos de carácter personal se refiere a una realidad que, más allá de constituir en sí misma un objeto de análisis de interés, afecta a múltiples disciplinas, teniendo, por lo tanto, un efecto transversal que lleva a que sea estudiada desde diferentes perspectivas. Los primeros estudios se dedicaban a

investigar fundamentalmente el sentido, significado y contenido del derecho, discutiendo, la mayoría de veces, sobre la necesidad de configurarlo como un derecho fundamental autónomo. Con el tiempo los análisis se han ido multiplicando y centrando en aspectos más concretos, teniendo en cuenta que la aplicación de las nuevas tecnologías en los diferentes ámbitos de la vida plantea problemas concretos que necesitan de investigaciones particularizadas. Precisamente esto es lo que aquí se propone, un trabajo dedicado a estudiar la protección de datos en un ámbito concreto como es el sanitario.

La mayoría de veces, cuando se hace referencia a la materia de protección de datos se piensa en el uso que las empresas que prestan servicios de telecomunicaciones hacen de la información o en los riesgos que el empleo de Internet genera para los datos de carácter personal. Sin embargo, y gracias sobre todo a la incisiva labor de divulgación que las distintas agencias de protección de datos realizan, poco a poco la ciudadanía se ha ido percatando de la importancia de salvaguardar la facultad de controlar los datos que a cada uno conciernen en otros ámbitos de la vida: educación, telecomunicaciones, bancos, aseguradoras y, como no, los centros sanitarios.

La cuestión de la protección de datos en el ámbito sanitario está adquiriendo paulatinamente mayor relevancia. Las cada vez más frecuentes noticias que en los medios de comunicación se refieren a esta cuestión y los constantes adelantos científicos que se están llevando a cabo en materias como la genética, sitúan a menudo en el candelero el debate sobre la importancia de proteger la información de carácter personal en el ámbito sanitario. Además, no se puede obviar el hecho de que las personas otorgan por lo general especial relevancia a los datos relativos a su salud. En este sentido las personas guardan cierto recelo a la hora de hacer públicos detalles sobre su estado de salud físico o mental. Evidentemente, esta situación se refuerza cuando se trata de enfermedades especialmente estigmatizadas. Y si bien hasta hace poco la actitud de los pacientes ante un tratamiento sanitario podía ser la de dejar en manos de los profesionales todo lo referente a sus cuidados, sin cuestionar su comportamiento, hoy día los ciudadanos reclaman una mayor autonomía y poder de disposición no sólo de su cuerpo sino también de todo lo que les afecta. La posibilidad de controlar lo que sucede con los datos de cada uno tiene así una relevancia especial en el ámbito sanitario. Hay que tener en cuenta que cuando una persona acude a un centro sanitario desnuda su intimidad aportando datos sobre aspectos de su vida que probablemente no revelaría en otros espacios. Poder controlar lo que sucede posteriormente con esta información tiene pues una importancia considerable para la ciudadanía.

La relevancia que en la realidad está adquiriendo la materia de protección de datos en el ámbito sanitario requiere una respuesta desde el ámbito del Derecho. En este sentido cabe preguntarse si existe un marco jurídico claro y preciso que determine los principios que rigen la protección de los datos sanitarios, concrete los derechos que la ciudadanía tiene en este ámbito sobre sus datos y especifique cómo se han de manipular los datos de carácter personal en este sector. Estas cuestiones han de tener solución para que los usuarios de los sistemas sanitarios conozcan cuáles son sus derechos a este respecto, pero también para que los profesionales de la sanidad sepan en qué parámetros han de actuar cuando emplean información de carácter personal.

Se trata de una materia que no ha sido analizada en muchas ocasiones de manera exhaustiva, por lo que se entiende de interés dedicar una investigación al respecto, que se pretende sea en profundidad, para plantear soluciones a los problemas interpretativos que genera la actual normación que rige la protección de datos sanitarios. El trabajo que se presenta tiene como objetivo señalar cuáles son las normas que marcan el régimen jurídico que regula la citada materia y tratar de aclarar su contenido.

El título del estudio, “Los principios de la protección de datos aplicados en la sanidad”, responde al hecho de que se analizará básicamente la regulación que en el título segundo de la LOPD se realiza de lo que en la Ley se califica como “Principios de la protección de datos”, si bien se hará una referencia también a los “Derechos de las personas” regulados en el título tercero. La Ley se divide en siete títulos. Pues bien, se atenderá sobre todo al contenido de los señalados, aunque en numerosas ocasiones habrá que hacer mención a cuestiones vinculadas a otros títulos. Esto se debe a que en los referidos apartados se regulan los aspectos nucleares del derecho a la autodeterminación informativa. Los citados principios y derechos conciernen a lo que se podría denominar, empleando conceptos clásicos aunque también cuestionados en la teoría general de los derechos humanos, “el contenido esencial” del mentado derecho. Ir más allá, analizando otras cuestiones, supondría llevar a cabo un trabajo desmedido que tendría como resultado un documento de una extensión cuyo manejo resultaría más complicado si cabe. Hay que tener en cuenta, además, que las más importantes particularidades o diferencias de la protección de datos sanitarios con respecto a la protección de datos en otros ámbitos se producen en ese núcleo, haciendo prescindible un análisis más extenso sobre otros puntos.

El trabajo se divide en seis capítulos. En el primero se tratará de contextualizar históricamente el debate que va a ser objeto de análisis. Se hará una breve referencia a las características principales de la Sociedad de la Información y se citarán proyectos políticos aportados desde diferentes ámbitos territoriales que tratan de potenciar su implantación en los diversos sectores de la vida. Se realizará también un pequeño estudio sobre los efectos que tiene la integración de las nuevas tecnologías en la Administración, subrayando el riesgo de control social que implicaría un mal uso de dichos instrumentos por los poderes públicos. En último lugar se profundizará en el concreto fenómeno de la telemedicina, otorgándole un significado concreto y subrayando las ventajas y desventajas que aporta este fenómeno. Asimismo, se hará una referencia a distintos instrumentos que se pueden considerar como ejemplos paradigmáticos de la telemedicina, para resaltar su importancia como nuevo modelo de práctica sanitaria. En definitiva se tratará de apuntar la importancia que en la actualidad tiene la información en prácticamente todos los sectores y en concreto en la sanidad, y subrayar el efecto de la incorporación de las TIC en este último ámbito como nuevo sistema de manipulación de datos que conlleva una mejora en la consecución del fin último de proteger la salud de las personas.

En el segundo capítulo se intentarán aclarar una serie de puntos que se estima necesario despejar, para afrontar después con una perspectiva más completa los aspectos nucleares del debate generado en torno a la protección de datos de carácter personal en el ámbito de la sanidad. Así, se intentará primero aclarar la importancia del Derecho en un ámbito tan complejo

como el de la protección de datos y se aportará un punto de vista sobre cuál ha de ser el papel de las normas a la hora de regular el uso de las nuevas tecnologías. En segundo lugar, se hará una breve referencia orientativa a las normas que se van a emplear a lo largo de este trabajo y que regulan la protección de datos sanitarios, y se hará hincapié en los argumentos que llevan a justificar la necesidad de aprobar una norma específica dedicada a regular esta materia. Tercero, y adentrándose en conceptos recogidos expresamente en la LOPD, se analizará la posibilidad que prevé la Ley de aplicar su contenido a los ficheros manuales, la importancia de esta consideración en el ámbito sanitario y los requisitos necesarios para que esta aplicación se produzca. Cuarto, se intentará aclarar un concepto tan importante como el de "tratamiento", teniendo en cuenta que el régimen jurídico recogido por la normativa de protección de datos entra en juego siempre y cuando los datos de carácter personal sean susceptibles de tratamiento. Este concepto habrá que distinguirlo de otros que también son empleados por la LOPD en su articulado, sobre todo del de recogida. Por último, se dará una definición del concepto "dato de carácter personal sanitario" y se analizará cuál es la consecuencia de que este tipo de dato tenga en las leyes la categoría de información sensible. El estudio de este último punto se llevará a cabo de forma escalonada partiendo del concepto de dato de carácter personal, analizando después lo que se debe entender por dato de salud y desgranando por último lo que implica que una información sea considerada sensible.

En el tercer capítulo la investigación se adentra en la interpretación de uno de los componentes más importantes del derecho a la autodeterminación informativa, como es el que configuran los principios de calidad de los datos. Se verá que toda manipulación de datos deberá respetar una serie de principios, que garantizan que ese uso se hará siempre de acuerdo a unos criterios que aseguran un mínimo control sobre los datos. Se trata de tres principios diferentes aunque inevitablemente relacionados. Primero se verá el principio de finalidad, que exige que cuando unos datos se recaban para cumplir con determinado fin éstos no puedan emplearse después para un objetivo diferente. La importancia de especificar el fin que se persigue deriva del hecho de que dependiendo del mismo el régimen jurídico aplicable al tratamiento de datos será distinto. En el caso que aquí se estudia los datos se manipulan para proteger la salud. Se tratará, por lo tanto, de dar un contenido específico a ese concepto. Segundo, se analizará el principio de pertinencia, que no es otra cosa que la concreción del tan conocido principio de proporcionalidad en el ámbito de protección de datos, y que exige que cuando se manipula información de carácter personal sólo se utilicen los datos estrictamente necesarios para el cumplimiento del fin pretendido. Tercero, se atenderá al principio de veracidad, que exige que los datos que se manipulan para la consecución de un fin reflejen la realidad, de tal forma que la información falsa deba ser rectificada o, en su caso, cancelada. La importancia de atender a estos principios en el ámbito sanitario deriva de la necesidad de que haya una coherencia entre el tratamiento de datos que se va a llevar a cabo y el fin que se pretende conseguir, ya sea la asistencia médica, llevar a cabo una investigación, realizar un estudio epidemiológico.

En el cuarto capítulo se analizará una figura de particular relevancia, por cuanto constituye, como ha subrayado gran parte de la doctrina, la principal facultad de control de una persona sobre sus datos. Se trata del consentimiento informado. Todo tratamiento de datos ha de estar justificado y el principal motivo de justificación será la autorización del titular de los datos. En

principio una manipulación de datos no puede llevarse a cabo sin el consentimiento informado de su titular. Sin embargo, esto no siempre es así. En este capítulo se tratará de aportar una interpretación de hasta dónde llega la capacidad del titular de controlar sus datos en el ámbito sanitario. Hay que tener en cuenta que en este sector es necesaria la manipulación ágil y sencilla de la información para que la actividad sanitaria sea lo más eficiente posible en el cumplimiento de sus fines, de tal manera que será necesario plantearse si se puede utilizar la información sin tener que recabar el consentimiento informado del titular. La LOPD regula el derecho a ser informado y el derecho a otorgar el consentimiento en apartados separados y así se hará también en este trabajo. Como se verá, ambas figuras se sujetan a regímenes jurídicos diferentes y plantean problemas específicos a la hora de aplicarse en el ámbito sanitario.

En el quinto capítulo, el más extenso, se atenderá a la cuestión que probablemente mayor polémica genera al analizar la protección de datos sanitarios. Se está haciendo referencia al estudio de los supuestos en que estos datos que están siendo manipulados en un ámbito concreto son transmitidos fuera de dicho espacio. Evidentemente uno de los principales riesgos objetivos, y también de los mayores miedos de la ciudadanía, en lo que concierne al ejercicio del derecho a la autodeterminación informativa en el ámbito sanitario, lo constituye que los datos sean transmitidos a sujetos distintos de los que inicialmente recibieron la información del titular. Existen diversas formas de que estas transmisiones se produzcan: la cesión, la vulneración del deber de secreto, lo que en la LOPD se denomina acceso a los datos por cuenta de terceros y la transferencia internacional. En un primer apartado se analizará la figura de la cesión y se hará también una referencia a la vulneración del deber de secreto. Ambas figuras se sujetan a un régimen jurídico semejante. Partiendo de la normativa de protección de datos, normativa sanitaria y otras normas que regulan aspectos sectoriales de la realidad se tratará de concretar cuándo y en qué condiciones pueden transmitirse los datos sanitarios a otros sujetos concretos o al público en general, para cumplir fines diversos. Se atenderá en un segundo apartado a una figura que cada vez tiene mayor relevancia en el ámbito de la protección de datos. El *outsourcing* o la externalización de servicios es una operación que se realiza actualmente con regularidad tanto en empresas privadas como en el seno de las administraciones y consiste en trasladar a un sujeto la tarea de llevar a cabo un servicio determinado en nombre del contratante. Muchas veces lo que se externaliza es la gestión de bases de datos u otras funciones que conllevan la manipulación de datos de carácter personal. Estas operaciones se llevan también a cabo en el ámbito sanitario por lo que se estima necesario realizar un análisis de las características que han de guardar para garantizar en todo caso el derecho a la autodeterminación informativa de los titulares de los datos que se transmiten. En el tercer apartado del capítulo quinto se atenderá a la figura de la transferencia internacional. Se trata de una operación que no se recoge en la LOPD dentro de los títulos dedicados a los principios de protección de datos y a los derechos, y que no ha sido analizada, salvo contadas excepciones, en profundidad por la doctrina. A pesar de que en el ámbito sanitario sea todavía una operación que no se produce con demasiada frecuencia, se considera aquí de interés estudiar, aunque sea de forma breve, uno de los tratamientos que mayores riesgos produce. Piénsese en la inseguridad que produce imaginar que los datos de salud de una persona puedan acabar en los ficheros de un responsable situado en un país que no cuenta con un sistema de protección de datos adecuado y que permite que esa información sea manipulada con gran laxitud.

En el sexto capítulo, el último, se analizarán los problemas interpretativos que genera la aplicación de los preceptos de la LOPD que regulan los derechos de las personas en el ámbito sanitario. Los derechos que serán objeto de estudio serán aquéllos cuya aplicación presenta ciertas particularidades en el ámbito sanitario: los derechos de acceso, cancelación, rectificación, oposición, a impugnar valoraciones y a una indemnización. Estos derechos constituyen un cuerpo de facultades de relevancia para el titular de los datos por cuanto le permiten llevar a cabo un control activo sobre lo que sucede con sus datos. Se hará una especial referencia a los tres primeros por ser los que se ejercen principalmente en el ámbito sanitario y los que provocan mayores problemas interpretativos. En este capítulo se tratará de averiguar hasta dónde puede llegar el ejercicio de estos derechos en el ámbito sanitario y si existen motivos que justifiquen su limitación.

El sistema a emplear en la investigación será fundamentalmente el que sigue. Teniendo en cuenta que se pretenden analizar los problemas que plantea la aplicación de la normativa de protección de datos en el ámbito sanitario, será necesario atender a esas dos realidades o disciplinas. Por lo general, a la hora de abordar los distintos puntos objeto de estudio en este trabajo se observará primero la regulación que la normativa de protección de datos realiza al respecto con el fin de hacerse con una visión periférica, para después acercarse desde una perspectiva más concreta al análisis de las dificultades que plantea la aplicación de esa regulación en el ámbito sanitario. Por último se tratará de aportar una interpretación de la normativa que entra en juego en la regulación de la materia que aquí se estudia, con el objetivo de proponer soluciones a los distintos conflictos entre intereses a los que se irá haciendo referencia. Lógicamente, estas propuestas, aunque basadas en Derecho, admiten discusión y podrán ser cuestionadas.

CAPÍTULO 1. TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN, SOCIEDAD, ADMINISTRACIÓN y SANIDAD.

Es costumbre inveterada comenzar los trabajos relacionados con los más diversos aspectos vinculados a la protección de datos de carácter personal con una referencia a la relevancia de la telemática en las sociedades actuales. Es una cuestión que ha sido expuesta en numerosas ocasiones por la doctrina. Se hará lo propio en el presente estudio. No se va a profundizar en aspectos que son sobradamente conocidos, pero sí subrayar una serie de puntos que ayuden a comprender el alcance de la materia que se va a tratar.

En este primer capítulo se expondrá el contexto histórico-social en el que se sitúa el debate sobre los problemas que surgen de la aplicación de la normativa de protección de datos al ámbito sanitario. Para una interpretación correcta de los principios que rigen dicha protección es preciso comprender primero los cambios que en la actualidad están viviendo las sociedades tecnológicamente avanzadas.

I. HACIA LA SOCIEDAD DE LA INFORMACIÓN.

La Historia de la Humanidad está compuesta por distintas etapas que se unen por eslabones de cambio, espacios de tiempo en los que uno o varios factores hacen que distintos aspectos de la vida se vean inmersos en un proceso de transformación. Antes fueron la rueda, la máquina de vapor, la electricidad, la imprenta, y ahora son las TIC: el teléfono, el ordenador, internet, etc. las que sitúan a la sociedad en uno de esos intervalos que dan paso a una nueva etapa[1].

I.1. El cambio ya está aquí.

La “Galaxia Gutemberg” ha muerto y la civilización se acerca a la consolidación de lo que se ha venido en llamar “la Sociedad de la Información”. Tal como se ha puesto de manifiesto por los propios tribunales la humanidad se encuentra inmersa en un nuevo mundo de constante transformación[2].

Muchos han sido los factores que a lo largo del tiempo han supuesto cambios en distintos aspectos de la vida. Sin embargo, ha habido algunos que han acarreado alteraciones más radicales en las estructuras de las sociedades y que han constituido verdaderas revoluciones. Pues bien, no se puede negar que actualmente se esté asistiendo a una auténtica revolución, a una alteración, cuando no ruptura, de los anteriores parámetros en los que se desenvolvía la vida. Se ha llegado a afirmar que se está ante algo más grande que una revolución: ante una

[1] CASTELLS, *La Era...*, cit., 1997, (volumen I), analiza este cambio; PÉREZ GÁLVEZ, “Administración sanitaria...”, cit., 2003, pone de manifiesto el salto que se ha dado estos últimos años: “El siglo XX se ha marchado y con él todos los anteriores de la denominada <<Galaxia Gutemberg>>. Hemos entrado en el infolito”.

[2] STS 3 de noviembre 1997, FJ. 10: donde se señala que “estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio sobre la realidad documental”.

nueva etapa de la humanidad, más importante aún que la revolución industrial o la aparición de la imprenta[3]. Se trata de la "Revolución de las TIC", de la etapa del simio informatizado[4].

Las TIC están cambiando prácticamente todos los aspectos de la vida[5]. En el ámbito político se está hablando ya de una nueva forma de participación ciudadana: la *living-room democracy*, ciber-democracia o tele-democracia, que permite al ciudadano la participación directa, a distancia, en los asuntos públicos, lo cual se espera que acarree una mayor implicación de éste en la vida política[6]; desde el punto de vista social la aportación de las TIC es incuestionable: Internet constituye una nueva sociedad, una plaza pública a la que todos y todas tienen acceso en libertad para relacionarse y organizarse; en cuanto a la cultura se puede decir que constituyen un medio inmejorable para la divulgación de la misma, e incluso puede afirmarse que con las nuevas tecnologías nace una nueva corriente cultural, la de los cibernautas; la influencia en el ámbito laboral es evidente al suponer las TIC un apoyo necesario para la realización de todo tipo de tareas[7], tanto desde el aspecto de la producción como de la gestión[8]; en el campo económico la transformación es también innegable, pues las TIC, además de constituir un instrumento imprescindible en los tres sectores hasta ahora conocidos, forman ya un nuevo sector económico generado en torno a la información y su tratamiento en continuo crecimiento[9].

Las nuevas tecnologías sitúan, como no podía de ser de otra forma, a las sociedades ante nuevos retos o problemas. El riesgo del desempleo por la sustitución de la persona por la máquina, la aparición de nuevas enfermedades como el aislamiento, la "brecha digital", el riesgo de control social, el peligro de homogeneización cultural, el surgimiento de nuevas formas de delito, etc. constituyen los principales riesgos que ha de afrontar la nueva sociedad de la información[10].

Estos problemas se concretan en multitud de situaciones en que los derechos y libertades de las personas pueden verse afectados negativamente. En lo que toca a los derechos a la intimidad y la autodeterminación informativa pueden ponerse diferentes ejemplos. En distintos ámbitos, caso del laboral, se ha puesto de manifiesto por los tribunales la posibilidad de que la

[3] OROZCO PARDO, "Notas acerca...", cit., 1998, p. 899, apunta cómo las TIC encarnan un cambio mayor que el que en su día supuso la creación de la imprenta, debido a que las Nuevas Tecnologías llegan a todas las esferas de la vida, incluso personal.

[4] TÉLLEZ AGUILERA, *Nuevas Tecnologías...*, cit,. 2001, p. 22.

[5] MUÑOZ MACHADO, *La regulación de la red…*, cit., 2000, p. 11; DEL PESO NAVARRO y RAMOS GONZÁLEZ, *La Seguridad…,* cit., 2002, p. XXXI.

[6] Dictamen ADPCat. CNS 3/2010, analiza las ventagas del voto electrónico.

[7] TASCÓN LÓPEZ, *El Tratamiento por la Empresa…,* cit., 2005, p. 59; DAVARA RODRÍGUEZ, *Manual de Derecho…,* cit., 2005, p. 35.

[8] CARDONA RUBERT, *Informática y Contrato…,* cit., 1999, p. 19.

[9] La facturación del mercado mundial TIC ascendió en 2008 a 2,67 billones de euros, un 4,6% más que en 2007, según el Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI) "La Sociedad en Red, 2009, http://www.ontsi.red.es. PÉREZ LUÑO*, Manual de Informática...*, 1996, pp. 98-99, pone de manifiesto la creciente importancia que el sector cuaternario constituido por la información está alcanzando, y cómo a las industrias del saber y de la información les corresponde una proporción cada vez mayor del producto nacional de los Estados con mayor índice de progreso.

[10] REESE, KUBICEK, LANGE, LUTTERBECK y REESE, *El Impacto...*, cit., 1982, y CASTELLS, *La Era...,* cit., 1997, exponen los efectos que las nuevas tecnologías tienen en las sociedades actuales. STEDH 2 de diciembre de 2008, K. U. v. Finlandia, FJ. 22: en la que se apunta que "El rápido desarrollo de las tecnologías de las telecomunicaciones en las últimas décadas ha dado paso a la aparición de nuevos tipos de delitos".

incorporación de las nuevas tecnologías se convierta en una vía para crear nuevas formas de control de la actividad de los ciudadanos, en este caso de los trabajadores, que no respeten la intimidad de los mismos[11]. Desde un punto de vista más general, se ha señalado como uno de los principales problemas del empleo de las nuevas tecnologías el alto riesgo de que se produzcan robos o suplantaciones de identidad en las actividades a realizar en el ciberespacio. El uso de una identidad electrónica en la realización de diversas tareas lleva a tener que salvaguardar en todo momento la veracidad o autenticidad de dicha identidad, garantizando que se asocia con una persona concreta. Las TIC generan un entorno en que dicha asociación no siempre es sencilla[12]. Otro aspecto problemático que se ha puesto de manifiesto en numerosas ocasiones ha sido el referido al tráfico de datos con los más diversos fines, como el comercial, vía *mailing*, que se ve facilitado por el uso de las nuevas tecnologías[13].

En términos generales, resulta hoy día comúnmente asumido que las nuevas tecnologías plantean nuevas dificultades o retos en materia de protección de derechos y libertades[14]. Sea para bien o para mal lo cierto es que la "tercera ola de Toffler"[15], la tercera gran revolución, ha llegado. El salto todavía no se ha consumado, no se ha consolidado la transformación y ciertamente no se sabe con seguridad a dónde va a llevar[16], y es que el cambio no es ni mucho menos un proceso meditado[17]. Sin embargo, la rapidez con que las TIC se están incorporando a los hogares, las empresas y las Administraciones públicas hace pensar que en no demasiado tiempo se pueda hablar de una sociedad de la información plena, en la que el uso de las TIC se convierta en algo cotidiano para todos y todas[18]. De hecho, se puede afirmar que las últimas dos

[11] STSJ de Andalucía, 9 de mayo de 2003, FJ 1, que subraya que "El desarrollo de las nuevas tecnologías, en especial de los sistemas y medios informáticos y telemáticos, está provocando nuevos e interesantes problemas jurídicos. Noticias de prensa y estudios doctrinales recientes se refieren a distintos conflictos con la intimidad que el uso de estas herramientas tecnológicas suscita en los más diversos ámbitos de la vida de los ciudadanos, destacando entre ellos el de la relación de trabajo o empleo. Basta con recordar los más actuales y palpitantes problemas como la realización de exámenes médicos, la utilización o revelación de datos de este tipo, el control de comunicaciones , correos electrónicos o similaries y los registros del ordenador"; STSJ de Navarra 27 de octubre de 2004, FJ 6: "la introducción de las nuevas tecnologías en el mundo laboral ha ayudado a reforzar la visión paóptica de la relación de trabajo; como muy gráficamente se ha llegado a decir, dichas tecnologías están reforzando el <<ojo electrónico>>, haciéndolo penetrante, dominante y ubicuo".

[12] STS 9 de mayo de 2007, en la que se analiza el caso en que una persona se identifica ante un sistema informático como una persona que no es en realidad, con el objetivo de conseguir una transferencia patrimonial; STS 12 de junio de 2007, en la que se analiza el caso en que diferentes sujetos se hacen pasar en la Red por trabajadores de un determinado banco para recabar cierta información con la que sustraer dinero a sus clientes. VVAA, *Robo de identidad…,* cit., 2010; ALAMILLO DOMINGO, "La identidad electrónica…", cit., 2010, p. 37.

[13] RUIZ CARRILLO, *El Tratamiento…,* cit., 2008, p. 28.

[14] PÉREZ LUÑO, "Derecho y nuevas tecnologías…", cit., 2005, p. 227.

[15] TOFFLER, *La Tercera...*, cit., 1980.

[16] VERDÚ, *Las Autopistas...*, cit., 1995, p. 108, afirma que "nunca la cocina de predicciones sociales estuvo más surtida de recetas sobre el porvenir".

[17] LEÓN, *El Papel...*, cit., 2002, p. 69, recoge las palabras de Keynes: "el futuro no se ve se hace", para poner de manifiesto el carácter irreflexivo de este proceso: el futuro se va haciendo sin que meditemos sobre él, sin que lo veamos primero.

[18] ORTEGA Y GASSET, *La Rebelión...*, cit., 1981, decía que hay épocas en que la trasformación de la realidad humana se acelera a velocidad veriginosa. Ciertamente, es innegable que nos encontramos en una de esas etapas.

generaciones se han convertido ya en el primer eslabón del *homo ciberneticus*[19], que tiene las nuevas tecnologías como extensión de su propio cuerpo.

I.2. La Sociedad de la Información.

No es fácil determinar cuál es la causa del nacimiento de esta nueva sociedad. Por un lado, parece claro que la necesidad de manipular grandes cantidades de información de forma ágil y segura, sobre todo en el ámbito público, ha impulsado el desarrollo de las nuevas tecnologías y el acercamiento a las TIC[20]. Sin embargo, no se puede negar que el mercado ha tenido mucho que ver en la popularización y socialización de dichos instrumentos y, por lo tanto, en la creación y posterior desarrollo de la sociedad de la información. Probablemente, lo más acertado sea afirmar que es la interacción de distintos factores la que ha llevado a las sociedades tecnológicamente más avanzadas al punto de desarrollo donde ahora se encuentran[21].

La doctrina que se ha dedicado a analizar los antecedentes, las causas, la evolución y las características de la sociedad de la información es realmente abundante. Para los fines que se pretenden basta aquí con acercarse a su significado y apuntar los rasgos principales que caracterizan a este nuevo fenómeno.

La sociedad de la información supone una nueva forma de organización en la que la información y las nuevas tecnologías que permiten el tratamiento y la transmisión de la misma, las TIC, fundamentalmente Internet[22], juegan un papel central[23]. Se ha definido como "un estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y Administraciones Públicas) para obtener y compartir cualquier información, instantáneamente, desde cualquier lugar y en la forma que se prefiera"[24].

La información siempre ha sido un elemento esencial para el desarrollo de las sociedades: donde hay organización hay información. Es más, se ha apuntado la información como uno de los componentes fundamentales de la naturaleza, junto a la materia y la energía, para el

[19] BALLESTERO, *La Brecha...*, cit., 2002, p.27, se hace eco de la reflexión de Toffler que reconoce que "somos la ultima generación de una antigua civilización y la primera de una nueva civilización".

[20] LEÓN, *El Papel...*, 2002, p. 73, afirma que han sido las necesidades de la sociedad las que han empujado a la creación de las TIC. Sin embargo cabe preguntarse si la popularización de las TIC en la sociedad se debe exclusivamente a la necesidad, o si, por el contrario, la promoción que en el mercado se ha realizado de esas nuevas tecnologías ha sido el detonante de la generalización del uso de esas tecnologías. Es cierto que la complejidad a la que han llegado las sociedades actuales ha hecho que sean necesarios instrumentos de tratamiento de información muy avanzados en sectores como la Administración Pública, sin embargo, que esa necesidad existiese en la sociedad civil no está tan claro.

[21] CASTELLS, *La Era,* cit., 1997, p. 31.

[22] FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías…*, cit., 1998, p. XX; MUÑOZ MACHADO, *La regulación de la red…*, cit., 2000, p. 19; PÉREZ LUÑO, "Derecho y nuevas tecnologías…", cit., 2005, p. 230, subrayan que Internet se ha convertido en el centro de la sociedad de la información.

[23] TONIATTI, "Libertad Informática..*",* cit., 1991, p. 140; FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías…*, cit., 1998, p. XX.

[24] Definición extraída del "Informe de Telefónica sobre la Sociedad de la Información", en http://www.telefonica.es/. La carácterística de la actual Sociedad de la Información es que si bien hasta ahora "la técnica (...) ha venido colaborando al desarrollo social (...), a partir de ahora, la sociedad está inmersa en las Nuevas Tecnologías, componente estructural de su ser y desarrollo mismo". Palabras de ORTEGA Y GASSET, recogidas en el Prólogo de ALVAREZ CIENFUEGOS, en la obra, SÁNCHEZ CARO y ABELLÁN, *Telemedicina y Protección...,* cit., 2002.

desarrollo de los pueblos[25]. Lo que ocurre en la actualidad es que la materia y la energía están siendo desplazadas por la información, que pasa a tener un papel central en todos los aspectos de la vida[26]. Este paso se ha dado porque la complejidad de las actuales sociedades hace necesario un manejo continuo de un volumen ingente de información[27] y porque a partir de la década de los cuarenta, cuando nace el primer ordenador, y sobre todo a partir de finales de los sesenta, cuando Internet empieza a dar sus primeros pasos, esta información ha encontrado la tecnología que permite manipularla de acuerdo con estas nuevas necesidades; es decir, se ha topado con la tecnología que le es más congenial[28]. En efecto, en los últimos 60 años los avances en materia de TIC se han ido sucediendo a una velocidad realmente asombrosa, y lo que es más importante, se han socializado con una rapidez desconocida hasta la actualidad con otras creaciones o invenciones[29].

En la base de esta revolución tecnológica se encuentran fundamentalmente dos fenómenos. Por un lado, está la unión entre la informática[30] y las tecnologías de la comunicación, lo que se ha llamado la telemática[31]. Por otro, está la digitalización, que permite que voz, imagen y datos viajen por el mismo medio convertidos en simples combinaciones de ceros y unos[32]. Estos dos procesos han posibilitado la realización de operaciones hasta ahora desconocidas, como enviar mensajes de texto, canciones o vídeos al otro lado del mundo en un instante. Si a todo esto se une que dichas operaciones se pueden realizar cada vez más rápido y que el coste de estas nuevas tecnologías no es exagerado para el ciudadano medio, se estará ante el escenario ideal para el desarrollo de la sociedad de la información.

Las posibilidades que ofrecen estas tecnologías son incalculables. Antes sólo se han apuntado unos ejemplos de los cambios que pueden traer en algunos ámbitos de la vida. Sin embargo, el mayor cambio lo supone, no la alteración de algunos aspectos en el trabajo o en la relación con la Administración, sino, en su conjunto, la transformación de las dimensiones

[25] DE MIGUEL CASTAÑO, "Libertad de Información..*",* cit., 1986, p. 168.
[26] DORMIDO BENCOMO, "Tecnologías de la Información...", cit, 1998, p. 57.
[27] DORMIDO BENCOMO, "Tecnologías de la Información...", cit., 1998, p. 73.
[28] TONIATTI, "Libertad Informática...", cit., 1991, p. 141; GUERRERO PICÓ, *El Impacto de Internet…*, cit., 2006, p. 329, señala Internet como "buque insignia de la globalización y de la Sociedad de la Información".
[29] Un claro ejemplo de lo afirmado es lo que ha ocurrido con el paradigma de las TIC, Internet, que nació en 1969 como ARPANET (*Advanced Research Projects Agency Network*), con fines exclusivamente militares, y que a partir de 1991, cuando se lanzó para uso de los ciudadanos , ha conquistado cotas de usuarios extraordinarias. En el Estado español, se ha pasado de 242.000 usuarios de internet en 1996, a 12.042.000 en 2004, es decir, del 0'7% de la población al 33'1%. En 2009, el porcentaje de hogares conectados a Internet es del 54 %. Sin embargo, esta cifra sigue estando por debajo de las cifras de EEUU, que contaba el 2002 con un 59% de la población como usuario, o Holanda con un 60%, o Suecia con un 62%. Datos extraídos de http://www.aui.es/ e Informe Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI), "La Sociedad en la Red", 2009. FERNÁNDEZ ESTEBAN, *Nuevas tecnologías…,* cit., 1998, p. 24; CONDE ORTIZ, *La Protección de Datos…,* cit., 2005, pp. 13-15.
[30] Con el término "informática" se hace referencia a la posibilidad de tratar la información de forma automática. CASTELLS, "Aproximación a...", cit., 1986, p. 27.
[31] VANDERBERGME, "Law and Information...*",* cit., 1989, p. 2: "*The word telematics is another French creation which encompasses the combination of informatics and telecomunications technology*"; FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías…*, cit., 1998, p. XX.
[32] Hay autores que han considerado que ha sido la digitalización de la información la verdadera clave de todo este proceso. Así FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías...*, cit., 1998, p. XIX; MUÑOZ MACHADO, *La regulación de la red…*, cit., 2000, p. 19.

fundamentales de la vida humana: el tiempo y el espacio[33], o cuando menos el hacer creer al usuario que rompe esas barreras del mundo real de una manera más radical que el teléfono o el avión[34].

Las nuevas tecnologías permiten realizar operaciones en un tiempo record[35], incluso al instante. Cada vez se compran equipos más rápidos que permiten tratar y transmitir información en cualquier formato a mayor velocidad. Por otro lado, Internet, como red de redes, permite una comunicación a nivel mundial que trae consigo un efecto globalizador en todos los sectores: las comunicaciones, las economías, las culturas, incluso las políticas se globalizan[36]. Los límites espaciales han perdido su sentido. El pueblo, la región, la villa, el cantón, la comunidad autónoma, el Estado, pierden en buena parte su razón de ser en este mundo interconectado[37], en la denominada aldea global. Es más, se llega a afirmar que el espacio, tal como se conoce en los parámetros de la realidad física, desaparece con las TIC dando lugar a un entorno virtual denominado "ciberespacio"[38]. Cuando se navega por Internet se está en el ciberespacio, cuando se habla por teléfono o se manda un correo electrónico se está en el ciberespacio[39], un entorno inmaterial en el que los átomos se transforman en bits[40].

El ser humano se ha construido una segunda naturaleza tan artificial como la luz eléctrica[41], o mejor, se ha separado de la naturaleza para crear un nuevo entorno donde desarrollar su nueva vida[42]. Este "tercer entorno" se constituye como un espacio de transmisión constante de información[43]. Se compra, se vende, se relaciona con otras personas, se tramita con la Administración, a través del intercambio de datos. Así pues, el denominado ciberespacio se constituye como una fuente inagotable de información.

[33] CASTELLS, *La Ciudad...*, cit., 1995, p. 21. En el mismo sentido la propia Ley Orgánica Reguladora del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD), 5/1992 de 29 de octubre de 1992, en su Exposición de Motivos recoge esta circunstancia al afirmar que el tiempo y el espacio, como límites, han desaparecido hoy gracias a las nuevas tecnologías.

[34] BARNÉS, "Una reflexión...", cit., 2000, p. 31.

[35] GARCÍA MEXÍA, "El Derecho...", cit., 2003, p. 86, pone de manifiesto la ruptura que Internet supone con "la servidumbre de respetar el inevitable transcurso de un cierto tiempo para ver ejecutados proyectos".

[36] MÉNDEZ RODRÍGUEZ, "Globalización de...", cit., 1999, p. 60: "En esa nueva sociedad de la información (informacional) existe una tendencia hacia la internacionalización de la tecnología que, cada vez más, se denomina tecno-globalismo. La aparición del término "globalidad" no es algo fortuito, es la gran metáfora con la que se describen las características del nuevo entorno informacional y económico (...): la tendencia hacia la globalización o mundialización de las relaciones políticas, económicas y mediáticas que caracteriza los intercambios entre los países en la última década de nuestro siglo. Unos intercambios que se sustentan en la existencia de redes de comunicaciones globales, en las autopistas de la información". LÓPEZ-ESCOBAR, "Comunicación, Participación...*",* cit., 2000-2001, p. 289: "El mundo se ha hecho más pequeño", se ha constituído un entorno sin barreras. La globalización es una realidad no sólo económica o política o cultural, también es una sensación, una convicción psicológica.

[37] VERDÚ, *Las autopistas...*, cit., 1995, p. 107.

[38] MOLES, PLAZA, *Derecho y Control...*, cit., 2004, p. 15: "El ciberespacio en sí mismo obviamente no es un territorio, es más bien un flujo de información que se configura en forma de red de comunicaciones".

[39] VERDÚ, *Las autopistas...*, cit., 1995, p. 107.

[40] NEGROPONTE, *El mundo...*, cit., 1995, en esta obra se analiza esta transformación.

[41] FROSINI, "El jurista...", cit., 1999, p. 242.

[42] PÉREZ LUÑO, *Nuevas Tecnologías...*, cit., 1987.

[43] ECHEVARRÍA, "Ética y Derechos...", cit., 2002, p. 223, habla del ciberespacio como un tercer entorno que se suma a los otros dos: naturaleza y ciudad.

La sociedad de la información se caracteriza por el papel preponderante que en ella toman los datos y la información. Todo tipo de actores (empresas, particulares e incluso la propia Administración) basan gran parte de sus actividades en recoger y manipular la mayor cantidad de datos posible con fines y medios tanto legítimos como ilegítimos[44]. La información se ha convertido en un bien preciadísimo, una mercancia que se vende, se compra, con la que se trafica[45]. Se ha asumido más que nunca que poseer información sobre personas, objetos o/y circunstancias, es tener poder, porque sitúa a su poseedor en una situación de privilegio[46]. La información siempre ha sido un bien preciado, pero en la actualidad las TIC han ejercido un efecto multiplicador en las posibilidades de acceso y manipulación de la misma.

En este entorno, hay que apuntarlo desde ahora, el riesgo de que los derechos a la intimidad y la autodeterminación informativa se vean afectados o atacados es mayor[47]. La especial relevancia que en la actualidad han adquirido los datos, sobre todo en el mercado, hace que los citados derechos fundamentales puedan verse en peligro con la generalización del uso de las TIC[48]. La posibilidad de que los flujos de información aumenten y que información proveniente de distintas fuentes se ponga en relación creando perfiles completos de los ciudadanos aumenta exponencialmente[49]. La sociedad de la información se fundamenta en una serie de instrumentos que mal empleados fortalecen el riesgo de que los ciudadanos pierdan el control sobre los datos que les conciernen.

I.3. Un apunte necesario sobre la brecha digital.

Quien no invierta en TIC se verá desplazado. Las empresas, los Estados e incluso las personas que no inviertan en nuevas tecnologías se verán fuera de la sociedad global informatizada. Se creará una brecha entre quienes tengan en su poder TIC y sepan manejarlas y los que no. Se habla, en este sentido, de la denominada "*digital divide*" o "brecha digital", que vendrá a ahondar en las desigualdades ya existentes entre el autodenominado primer mundo y el tercero. La falta de infraestructuras en TIC, la carencia de formación y la ausencia de medios

[44] Han sido muchos los casos de contrabando de información. Podemos poner como ejemplo dos casos paradigmáticos: "El comercio con datos de la Seguridad Social provoca la condena de un funcionario", Boletín de noticias LOPDate, 21/04/2004; pitonisas y videntes dedicadas a recabar datos personales con fines comerciales, Boletín de noticias LOPDate, 20/02/2003, en http://www.lopdate.com/.

[45] FERNÁNDEZ ESTEBAN, *Nuevas Tecnologías...,* cit., 1998, p. 139: "Las nuevas tecnologías convierten la información en una riqueza fundamental de la sociedad. Las tecnologías interactivas crean una nueva <<mercancía>>".

[46] SÁNCHEZ MECA, "Cuestiones eficaces...", cit., 1998, p. 451. "La libertad personal y las posibilidades de intervenir en los procesos sociales, económicos y políticos, están ahora muy determinados por el acceso y el control de la información". La consideración de Bacon de que hoy día el verdadero poder viene de la mano de la información y las TIC, y no de la fuerza física o del dinero ha sido sostenida multitud de veces por la doctrina. Por eso quien controle las TIC controlará el poder. CASTELLS, "Aproximación a la Problemática...", en *Jornadas Internacionales...,* 1986, p. 27; GUERRERO PICÓ, *El impacto de Internet…*, cit., 2006, pp. 343-344: "La compra y venta de datos personales está en alza"; MURILLO DE LA CUEVA, "La Construcción del Derecho…", cit., 2009, p. 58.

[47] MURILLO DE LA CUEVA, "La Construcción del Derecho…", cit., 2009, p. 16; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 45-46.

[48] GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, p. 408 y siguientes: realiza un riguroso análisis de los riesgos que para la privacidad supone el empleo, sobre todo, de Internet.

[49] VIZCAÍNO CALDERÓN, *Comentarios a la Ley…,* cit., 2001, p. 34; ARENAS RAMIRO, *El Derecho Fundamental…,* cit., 2006, pp. 33-34.

para acceder a ello plantean el riesgo de que se genere una fractura tecnológica que aísle, aún más si cabe, a las sociedades económicamente menos desarrolladas[50]. No hay más que ver los clásicos índicadores de integración en la sociedad de la información para observar que las desigualdades entre continentes son evidentes[51]. Las TIC que en principio son instrumentos de conexión, de unión, de comunicación, se pueden convertir en factor de división, no sólo entre ricos y pobres, sino también entre personas formadas y no formadas[52].

Evitar que las nuevas tecnologías se erijan en motivo de división entre los países económicamente desarrollados y subdesarrollados y hacer que se conviertan en un instrumento de desarrollo global tiene que ser un reto prioritario. Para ello, resoluciones como las adoptadas en la Cumbre Mundial sobre la Sociedad de la Información, que señalan las TIC como instrumentos de desarrollo y cooperación[53], no pueden caer en saco roto.

La efectividad de estos compromisos pasa fundamentalmente por asumir una premisa inicial. Se trata de la necesidad de situar a la persona, el factor humano, en el centro de la sociedad de la información. Es decir, de priorizar el aspecto humano sobre el mercantil, fijando las bases para que las nuevas tecnologías se desarrollen en un marco ético que se ha llamado el "humanismo tecnologíco"[54]. Se ha considerado por parte de la doctrina que la entrada en la sociedad de la información se está produciendo de la mano de intereses mercantilistas, antepuestos a los éticos[55]. La igualdad o la libertad no tienen preferencia en la práctica frente a los aspectos económicos. Frente a esta vía es necesario defender otra visión de la sociedad de la información, entendida como un entorno civilizado, democratizado y humanizado[56]. No se trata, ni mucho menos, de dar una visión idealista de lo que podría ser la nueva sociedad[57], sino de apuntar que las TIC no son, o no deben ser, meramente una cuestión de poder[58]. En definitiva, hay que recordar que en el centro de la nueva sociedad no puede situarse, aunque pudiera parecer una contradicción *in terminis*, la información, sino la persona. La información no puede ser un fin, sino un medio.

Está en manos de las personas el no convertir las TIC en instrumentos perversos[59]. No son las herramientas las que plantean problemas. Las nuevas tecnologías no son buenas ni malas

[50] BALLESTERO, *La Brecha...*, cit., 2002, p. 63 y siguientes.
[51] Mientras que en Norteamérica el 76% de los habitantes son usuarios de internet, en el continente africano esa cifra sólo alcanza el 12%. Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI), 2009, "La Sociedad en Red 2009", en http//www.ontsi.red.es
[52] CRIADO GRANDE y RAMILO ARAUJO, "e-Administración ¿un reto...", cit., 2001, p. 22.
[53] Cumbre Mundial sobre la Sociedad de la Información, fase de Ginebra, 10-12 septiembre 2003, y fase de Túnez, celebrada entre el 16 y 18 de noviembre de 2005, http://itu.int/wsis/index-es.html.
[54] DAVARA RODRÍGUEZ, *Manual de Derecho…*, cit., 2005, p. 42.
[55] DAVARA RODRÍGUEZ, *De las autopistas...*, cit., 1996, p. 23.
[56] ECHEVERRÍA, "Ética y Derechos...", cit., 2002.
[57] PÉREZ LUÑO, *¿Ciberciudadaní@ o...,* cit., 2004, y CASTELLS, *La Ciudad...*, cit., 1995, ponen de manifiesto lo simplista e inútil de planteamientos utópicos como la "computopía" de Masuda, o apocalípticos como los del *"Big Brother"* de Orwell.
[58] DEL PESO NAVARRO y RAMOS GONZÁLEZ, *La Seguridad…,* cit., 2002, pp. XXXIII-XXXIV.
[59] DRUMMOND, *Internet, Privacidad y Datos…*, cit., 2004, pp. 27-28.

per se. Es el uso que se les da las que las convierten en algo positivo o negativo[60]. Que esto sea así depende en gran parte de la iniciativa y de la voluntad de los gobiernos de todo el mundo[61].

I.4. Breve exposición de las iniciativas políticas para la implantación de la Sociedad de la Información.

En el ámbito europeo las primeras iniciativas dirigidas a fomentar políticas comunitarias promotoras de la investigación, la inversión y la producción en nuevas tecnologías surgen de manera temprana, ya en 1974[62]. El objetivo fundamental de dichas políticas era situarse a la cabeza del mundo en materia de nuevas tecnologías, tomando como bandera la ya comentada y cierta afirmación de que "la información es poder"[63].

Los proyectos políticos más amplios y relevantes que han marcado la vía a seguir a nivel europeo hasta la actualidad han nacido a tren de lo que se dictaba en EEUU. En septiembre de 1993 nace en EEUU el proyecto "*The National Information Infraestructure: Agenda for action*", impulsado por Al Gore y centrado en cuatro aspectos: los usuarios, la información, aspectos técnicos y económicos[64]. A la sombra de este plan se adoptó en Europa el 5 de diciembre de 1993 el "Libro Blanco sobre Crecimiento, Competitividad y Empleo: Desafíos y Oportunidades en el siglo XXI"[65]. Un año después, en mayo de 1994, vio la luz el conocido informe Bangemann[66], que sentó las bases del "plan e-Europe", que ahora está vigente y que tiene su nacimiento en diciembre de 1999 en una comunicación de la Comisión para el Consejo Europeo extraordinario de Lisboa de 23 y 24 de marzo del 2000, presentada en el Consejo Europeo de Helsinki del 10-11 de diciembre de 1999. Este documento planteaba tres objetivos principales: conectar a la red y llevar la era digital a cada ciudadano, hogar y escuela y a cada empresa y administración; crear una Europa de la formación digital, basada en un espíritu emprendedor dispuesto a financiar y desarrollar las nuevas ideas; y velar por que todo el proceso sea socialmente integrador, afirme la confianza de los consumidores y refuerce la cohesión social[67]. Para cumplir con estos fines reconocía la necesidad de llevar a cabo 10 diez acciones diferentes: dar acceso a la juventud europea a la era digital; abaratar el acceso a Internet; acelerar la implantación del Comercio electrónico; implantar una Internet rápida para investigadores y estudiantes; Tarjetas Inteligentes para el acceso seguro a las aplicaciones electrónicas; crear un entorno propicio para que las ideas se desarrollen comercialmente y sean financiadas dentro de la Unión para conseguir un máximo de capital-riesgo disponibles para las PYME de alta tecnología; la participación de los

[60] MURILLO DE LA CUEVA, "Avances Tecnológicos...", cit., 2003, p. 30.
[61] Informe final de la fase de Ginebra de la Cumbre Mundial sobre la Sociedad de la Información, 12 de mayo de 2004, http://www.itu.int/wsis/index-es.html.
[62] Resolución del Consejo, 15 de julio de 1974 sobre una Política Informática Comunitaria, Diario Oficial nº C-086 de 20/07/1974.
[63] MÉNDEZ RODRÍGUEZ, "Política del Tándem...", cit., 1999, p. 7; GÓMEZ NAVAJAS, *La protección…,* cit., 2005, p. 33.
[64] MÉNDEZ RODRÍGUEZ, "Política del Tándem...", cit., 1999, p. 7.
[65] *WhitePaper on Growth, Competitiviness, and Employment: the Challenges and Ways forward into the 21st century,* COM (93) 700 final. VELÁZQUEZ BAUTISTA, *100 Interrog@ntes...,* cit., 2004, p. 43.
[66] Informe Bangemann, *Recommendations to the European Council, Europe and the Global Information Society,* de 26 de mayo de 1994, http://europa.eu.int/.
[67] COM (1999) 687. Consejo Europeo de Lisboa, 23 y 24 de marzo del 2000, Conclusiones, en http://www.europar.eu.int/.

incapacitados en la cultura electrónica; el transporte inteligente; la Administración pública en línea. La concreción de este plan e-Europe se dio en el Consejo Europeo de Feira el 19-20 de junio del 2000 con la aprobación del "plan eEurope 2002 una Sociedad de la Información para todos"[68]. La finalidad de este plan era conseguir que el objetivo fijado en la cumbre de Lisboa se alcanzara. Este objetivo no era otro que convertir a Europa en la economía más competitiva y dinámica del mundo. Para ello focalizaba las líneas de acción establecidas por el plan inicial en tres: un internet más rápido, barato y seguro; invertir en las personas y en la formación; y estimular el uso de internet. En estas tres líneas de acción se englobaban 64 objetivos o acciones concretas. Además, se planteaban nuevas cuestiones como la necesidad de formar personal cualificado relacionado con la sociedad de la información; la necesidad de lograr una sociedad integradora; y la necesidad de suministrar contenidos digitales de calidad para internet.

La valoración de esta primera etapa del plan eEuropa fue positiva. En el informe final eEurope 2002, emitido por la Comisión el 11 de febrero de 2003[69], ésta se congratulaba de haber alcanzado la gran mayoría de los 64 objetivos: la conexión en los hogares, empresas y administraciones había crecido rápidamente en porcentajes muy altos; también la velocidad de la red; se había aprobado un marco jurídico que reforzaba la competencia en el mercado, y que se esperaba supusiera la reducción de precios, que garantizaba la libertad de elección del consumidor, etc.; había aumentado el uso de internet en escuelas y los servicios públicos en línea etc.. Sin embargo, en el informe se reconocía que quedaba mucho por hacer. De ahí la necesidad de un nuevo plan que completara el anterior. En el Consejo Europeo de Barcelona[70] se solicitó a la Comisión que elaborase un plan que diese continuidad o completase el plan eEuropa 2002. Este nuevo plan fue elaborado por la Comisión y aprobado en el Consejo Europeo de Sevilla[71]. Se trataba del denominado "Plan eEuropa 2005: una Sociedad de la Información para todos"[72]. El objetivo de este plan de acción era fomentar unos servicios, aplicaciones y contenidos seguros basados en una infraestructura de banda ancha ampliamente disponible. Para el 2005 Europa debía contar con unos servicios públicos en línea modernos: una Administración electrónica, unos servicios electrónicos de aprendizaje, unos servicios electrónicos de salud; y un entorno dinámico de negocios electrónicos; y para ello, con un acceso de banda ancha ampliamente disponible y a precios competitivos y una infraestructura de información segura. Sobre estos objetivos incide el actualmente vigente plan "i-2010", que se dirige a la consecución de un triple objetivo: la configuración de un espacio europeo único de la información, el impulso de la innovación y la inversión en el campo de las TIC, y la configuración de una sociedad de la información y los medios de comunicación basada en la inclusión. Para conseguir estos fines se plantean desde la UE múltiples acciones: aumentar la velocidad de los servicios de banda ancha, fomentar los nuevos servicios y los contenidos en línea, hacer que Internet sea segura, poner en marcha iniciativas de investigación, fomentar la inversión privada en investigación e innovación, definir políticas de comercio electrónico, adoptar un plan de acción

[68] COM (2000) 330 final.
[69] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social, y al Comité de las Regiones, COM (2003) 66 final.
[70] Conclusiones de la Presidencia-Consejo Europeo de Barcelona, 15-16 de marzo, 2002, en el punto 40.
[71] Conclusiones de la Presidencia-Consejo Europeo de Sevilla, 21-22 junio de 2002, punto 54.
[72] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social, y al Comité de las regiones, COM (2002) 263 final.

sobre administración electrónica y orientaciones estratégicas para estimular el uso de las TIC en los servicios públicos, etc[73].

Las iniciativas políticas que en los diferentes momentos se han ido aprobando a nivel europeo han subrayado la necesidad de que las nuevas tecnologías entren en los distintos ámbitos de la vida de los ciudadanos europeos y de que Europa se conecte a la red. El principal problema que encuentran las iniciativas europeas es la divergencia existente entre los distintos países de la UE en materia de implantación y uso de TIC. Las desigualdades entre los distintos países son evidentes. Mientras se pueden encontrar países completamente inmersos en los diferentes ámbitos de la sociedad de la información como Holanda, Dinamarca o Suecia, hay otros, entre los que se encuentra el Estado español, que tienen que realizar un esfuerzo mayor para acercarse a las cifras que presentan los países más avanzados[74].

Para acercarse a las cifras de los países tecnológicamente más avanzados en 2001 se dio entrada en España al Plan INFO XXI[75]. El objetivo de este plan era muy amplio: implantar la Sociedad de la Información en España para que todos sus ciudadanos y empresas pudieran participar en su construcción y aprovechar las oportunidades que ésta ofrece, con el fin de aumentar la cohesión social, mejorar la calidad de vida y de trabajo y acelerar el crecimiento económico. Para ello planteaba diez objetivos estratégicos, a saber: las tecnologías de la información tienen que estar al alcance de todos, la SI tiene que volcarse en la educación y la formación, la sociedad de la información tiene que sustentarse en unas infraestructuras y un marco legal propicios, tiene que promover la cultura propia, es objetivo fundamental mejorar la calidad de vida de los ciudadanos, facilitar la innovación y el desarrollo de las nuevas tecnologías, desarrollar el comercio electrónico y potenciar las empresas estatales, una Administración transparente y centrada en el ciudadano, promocionar el uso de las TIC por las empresas, y crear una sociedad más vertebrada en la que todos valgan.

Este plan recibió numerosas críticas, no tanto por su contenido sino por la falta de inversiones y por la lentitud en su cumplimiento[76]. Teniendo en cuenta que no se estaban alcanzando los objetivos marcados, se encargó un informe a una comisión de expertos que plasmó sus conclusiones en el conocido Informe Soto[77]. Se ponía de manifiesto en este informe que el ritmo de implantación de las nuevas tecnologías iba muy por detrás de la evolución de las posibilidades que ofrecían las mismas. Fijaba diez puntos clave para relanzar la Sociedad de la Información en España: elaborar un nuevo plan que sustituyera al INFO XXI, claro y realista; asegurar el liderazgo político; creación de una organización que se ocupara de la gestión del plan; desarrollar un plan de comunicación con la sociedad que emocionara a ésta; potenciar la formación; apostar

[73] Comunicación de la Comisión, 1 de junio de 2005, al Consejo, al Parlamento Europeo, al Comité de las Regiones titulada "i2010-una sociedad de la información europea para el crecimiento y el empleo".
[74] En el Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas, Avanza, se señala que España se sitúa por debajo de la media europea en relación al gasto realizado en TIC-s y la difusión y uso que éstas tienen, en http://www.planavanza.es.
[75] http://www.administración.es/
[76] En http://www.elmundo.es/navegante/ se pueden consultar numerosos artículos que ponen de manifiesto esta situación.
[77] "Aprovechar la Oportunidad de la Sociedad de la Información en España", Recomendaciones de la Comisión Especial de Estudio para el Desarrollo de la Sociedad de la Información, 1 de abril de 2003, http://cdsi.red.es/.

por la Administración electrónica; equiparar legalmente el mundo internet al físico; acelerar la entrada de los ciudadanos en internet; impulsar las TIC en las empresas; y, contribuir a la integración social.

Siguiendo las instrucciones del Informe Soto se aprobó el 11 de julio de 2003 el nuevo plan denominado "España.es: Programa de Actuaciones para el Desarrollo de la Sociedad de la Información en España"[78]. Se trataba de un programa más flexible que intercalaba proyectos a largo plazo con otros a corto plazo, actuaciones de carácter horizontal o general frente a actuaciones en segmentos concretos. Hoy día es el "plan avanza" el que marca las líneas maestras ha seguir para la completa integración de España en la sociedad de la información. En términos genéricos este plan constituye un proyecto integral que actúa en todos los sectores de la realidad. En un primer paso el plan avanza-1 actúa en el área de la ciudadanía digital, la economía digital, los servicios digitales y el contexto digital[79]. En un segundo paso, el plan avanza-2, que se incardina en un proyecto que se extiende hasta 2015, tiene como objetivos promover procesos innovadores TIC en las administraciones públicas, extender las TIC en la sanidad y el bienestar social, potenciar la aplicación de las TIC al sistema educativo y formativo, mejorar la capacidad y la extensión de las redes de telecomunicaciones, extender la cultura de la seguridad entre la ciudadanía y las empresas, incrementar el uso avanzado de servicios digitales por la ciudadanía, extender el uso de soluciones TIC de negocio en la empresa, desarrollar las capacidades tecnológicas del sector TIC, fortalecer el sector de contenidos digitales garantizando la mejor protección de la propiedad intelectual en el actual contexto tecnológico y dentro del marco jurídico español y europeo, y desarrollar las TIC verdes. Para ello se pretende incidir en cinco ejes de actuación: desarrollo del sector TIC, capacitación TIC, Servicios públicos digitales, Infraestructura y Confianza y Seguridad[80].

En lo que respecta a la Comunidad Autónoma del País Vasco es el Plan Euskadi en la Sociedad de la Información el que determina las líneas a seguir para la integración de Euskadi en la sociedad de la información. Ya en 1999, en el debate de política general, el entonces Lehendakari asumió el reto de la sociedad de la información ante el pleno del Parlamento Vasco, reto que se concretó en este plan. El objetivo era crear una Euskadi conectada, abierta, mirando al conocimiento, atractiva, basada en la solidaridad. Para ello se impulsó la actuación de todos los agentes: ciudadanos implicados, integrados y formados; la empresa como motor de la sociedad de la información; la Administración como referente, ejemplo y apoyo. Se trataba de crear una comunidad más culta, dinámica, socialmente más avanzada y cohesionada, donde la calidad mejorara constantemente y se generara riqueza. Las acciones giraban en torno a los ciudadanos, empresas y Administración, como en los demás planes, tratando de conseguir internet para todos, empresas informatizadas, Administración *on-line*, formación, e-sanidad, calidad en los contenidos, infraestructuras y tecnologías propicias, y un marco normativo adecuado. El Plan Euskadi en la Sociedad de la Información ha tenido su último impulso en 2010. La aprobación de la denominada "Agenda Digital de Euskadi" pretende constituir un importante

[78] http://www.mcyt.es/asp/ministerio_informa/prensa/pdf/Espana_es_Actuaciones.pdf/
[79] Plan 2006-2010 para el desarrollo de la Sociedad de la Información y de Convergencia con Europa y entre Comunidades Autónomas y Ciudades Autónomas.
[80] Estratategia 2011-2015, Plan Avanza 2, en http://www.planavanza.es.

eslabón en la integración de la CAPV en la sociedad de la información. Este proceso cuenta con diferentes líneas de actuación: ciudadanía activa, que pretende fomentar la sensibilización sobre la utilidad de las TIC, la participación de los ciudadanos en aras del bienestar individual y colectivo, y tiene como objetivo reducir la exclusión digital; empresa innovadora, que se dirige a maximizar el rendimiento de las nuevas tecnologías en el ámbito empresarial; servicios públicos digitales, que trata de avanzar o profundizar en la administración electrónica; euskadi.net, que se dirige a dar presencia a Euskadi en la red; infraestructuras, que trata de implantar los medios necesarios para acceder a la Sociedad de la Información, haciéndola llegar a cualquier punto[81].

De esta breve exposición fácilmente se deduce que, en términos generales, todos los proyectos coinciden en lo fundamental a la hora de marcarse los objetivos. El problema de los planes reside en su implantación en la práctica. Más allá de los problemas económicos, técnicos o jurídicos que pudieran derivarse de la incorporación de las TIC en las sociedades, la integración de las nuevas tecnologías en la vida cotidiana plantea un reto de envergadura. Una de las principales dificultades en esta labor la presenta la necesidad de que se produzca una evolución armónica de los distintos actores: empresa, poderes públicos y ciudadanía, en la adaptación a la nueva sociedad. Para que se produzca una exitosa evolución de la sociedad de la información es necesario que todos los agentes afectados se impliquen de igual manera en el proceso. Desde esta perspectiva resulta un lugar común afirmar que hoy día no parece que esta armonía guíe la evolución y desarrollo de la sociedad de la información. Mientras que las empresas y administraciones se dedican a crear nuevas herramientas para lanzar el comercio electrónico y crear nuevos servicios *on-line*, el ciudadano medio emplea las nuevas tecnologías con fines vinculados al ocio, sin explotar todas sus potencialidades en lo que se refiere a relacionarse con la Administración y participar en los asuntos públicos[82]. Si bien las administraciones y las empresas cuentan con un nivel de integración relativamente alto en la sociedad de la información, los ciudadanos se encuentran parcialmente integrados en este nuevo entorno, pues sólo emplean algunas de las aplicaciones de las nuevas tecnologías, utilizando principalmente los antiguos procedimientos para relacionarse con la Administración y las empresas. Los ciudadanos no parecen ser conscientes del cambio que puede suponer la incorporación plena de las TIC en su vida, de las ventajas que presenta y de los riesgos que plantea[83]. Sea por desconfianza, por inseguridad, por desconocimiento, o por falta de formación, lo cierto es que la ciudadanía está actuando como mero espectador en este proceso, en términos de algún autor, como "ciudadano.com"[84]. Esto lleva a que el avance de la sociedad de la información, en su conjunto, no sea el que en un inicio se podía esperar.

[81] http://www.innova.euskadi.net.

[82] "Se afianza la tendencia del uso personal de *Internet*". "Otro tipo de usos como son los trámites administrativos (...) apenas son utilizados por los internautas", en Informe del EUSTAT, *La Sociedad de la Información y las Familias*, del 2002, en http://www.eustat.es/ . En el mismo sentido el Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI), "La Sociedad en Red 2009", http://www.ontsi.red.es.

[83] DAVARA, "Hacia un nuevo...", articulo publicado en http://www.iee.es/.

[84] PEREZ LUÑO, *¿Ciberciudadaní@...,* cit., 2004, en esta obra distingue el autor entre el ciberciudadano, que participa activamente en la Sociedad de la Información, y el ciudadano.com, que no es más que un espectador.

II. LA ADMINISTRACIÓN ELECTRÓNICA.

II.1. La necesidad de incorporar las TIC a la Administración Pública.

En la búsqueda de la citada armonía el papel de la Administración puede resultar fundamental. Por un lado, el aparato público tiene que fijar los parámetros en los que se tiene que producir la transformación de la sociedad, concretando en planes los términos en los que se dará la integración de la sociedad en la "era de la información". Por otro, tiene que constituir un ejemplo de dicha integración incorporando a su funcionamiento las nuevas tecnologías, sensibilizando así a los demás agentes sobre la importancia del proceso en el que se está inmerso y haciendo posible que los demás agentes se relacionen con las administraciones empleando la telemática. El aparato público ha de ser ejemplo, no ya de incorporar las nuevas tecnologías a su funcionamiento, objetivo en gran medida logrado, sino de fomentar su uso como una herramienta de participación en los asuntos públicos, de realización de transacciones comerciales o de relación permanente entre administraciones y órganos diferentes.

Si bien es cierto lo dicho hasta ahora, la necesidad de incorporar las TIC en la Administración responde sobre todo a otro factor, más allá de su relevancia en la citada labor armonizadora. En este sentido, en la medida en que las sociedades han ido evolucionando los estados se han configurado como organizaciones cada vez más complejas y el aparato administrativo, como personificación del Estado, entendido en sentido amplio, ha ido tornándose a su vez en un cuerpo cada vez más complicado, no sólo a ojos del ciudadano, sino también *ad intra*, en su funcionamiento y organización.

En la actualidad, la asunción de un modelo de Estado como el de bienestar conlleva la carga del aparato público con nuevas tareas a realizar.[85] Las sociedades crean nuevos problemas que los ciudadanos exigen sean resueltos y, así, la Administración se ve obligada a renovarse para hacer frente a los mismos con eficacia[86]. Pues bien, detrás de cada nuevo problema o nueva tarea hay la gran mayoría de las veces nueva información que manipular, información que muchas veces se refiere a personas identificadas o identificables. Es así que uno de los mayores problemas a los que se enfrentan las administraciones lo constituye, más ahora que el proceso de descentralización funcional y de desconcentración de la Administración es mayor, la incapacidad de ésta para manipular con los viejos sistemas toda esta información. Ante esta afirmación resulta a día de hoy indudable la necesidad de integrar las TIC en el funcionamiento y organización de las administraciones, con el fin de que su actividad sea lo más eficaz posible[87].

[85] En posteriores capítulos se hará una breve referencia al significado de la consideración en la CE del Estado español como Estado social y democrático de Derecho. En cualquier caso, para tomar conciencia de lo que esta declaración supone ver PÉREZ LUÑO, *Derechos Humanos...*, cit., 1996.

[86] REESE, KUBICEK, LANGE, LUTTERBECK y REESE, *El Impacto....*, cit., 1982, p. 98, se hacen eco de esta situación al afirmar que "nuestra sociedad de crecimiento y consumo se encuentra sometida a un cambio constante, bajo cuyo influjo aumentan, que no decrecen, las tareas de las que tiene que hacerse cargo el Estado".

[87] PÉREZ LUÑO, *Manual de Informática...,* cit., 1996, pp. 83-84, concluye tajantemente que "dichas tareas, en los países industrializados sólo pueden llevarse a cabo adecuadamente con la ayuda de la informática (habría que decir telemática)" y que "la informática, al posibilitar la racionalización, simplificación, celeridad y seguridad de las prácticas administrativas se presenta como una exigencia implacable para cualquier Estado que no desee vivir de espaldas al progreso"; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 267-269.

La ingente cantidad de datos que las administraciones tienen que manejar sólo puede ser empleada de forma ordenada, sistemática y racional a través de las nuevas tecnologías, que permiten una rápida pero organizada y segura manipulación y transmisión de dicha información[88].

La necesidad de implantar las TIC en la Administración resulta evidente[89]. Los efectos que en su funcionamiento y organización puede tener la incorporación de las nuevas tecnologías resultan reconocibles. Primero, facilitan el tratamiento efectivo de la información, evitando la repetición de datos, su pérdida o alteración[90]. Segundo, posibilitan una comunicación vía intranet e internet rápida y fiable entre distintas administraciones o entre diferentes departamentos u órganos de una misma Administración, lo cual repercute a favor de la celeridad en los procedimientos y la colaboración.

Las ventajas del empleo de las TIC en el funcionamiento interno de las actuales administraciones son perfectamente visibles. No obstante, la necesidad de implantar las nuevas tecnologías en la Administración responde también a motivos de mayor entidad, vinculados a una nueva forma de entender la relación ciudadano-Administración[91]. En el ámbito externo la incorporación de las TIC supone un cambio esencial[92]. Además de mejorar los servicios que la Administración presta a los ciudadanos[93], las TIC traen consigo un replanteamiento de esa relación[94]. Las nuevas tecnologías, en especial Internet, hacen posible una comunicación directa, inmediata y continua entre estos agentes. Esta alternativa, además de agilizar el procedimiento administrativo, democratiza en cierta medida el funcionamiento del aparato público[95]. Foros de opinión, buzones de quejas, páginas *web* informativas, hacen que la Administración sea más transparente y cercana[96]. La Administración Electrónica no supone simplemente hacer lo mismo

[88] GAY FUENTES, *Intimidad y Tratamiento…,* cit., 1995, p. 17; DE ASÍS ROIG, "Documento electrónico...", cit., 1996, p. 130, apunta que "la Administración Pública es un centro de generación y gestión de información de una magnitud difícilmente equiparable con cualquier otro sujeto. Su función constitucional de satisfacción de los intereses generales determina la necesidad de conocer, elaborar, decidir y comunicar información que, a su vez puede ser tratada, archivada y gestionada con fines de interés general".
"No es por ello de extrañar que la Adminsitración tenga un especial interés en aprovechar las oportunidades de rapidez de manejo, magnitud de información y fiabilidad que ofrecen los diversos sistemas de tratamiento de la información y así se considera que su definitiva incorporación a la actividad administrativa constituya un punto clave en su proceso de modernización".

[89] GARCÍA-POGGIO*, "*Hacia una nueva...", cit., 1998, p. 9; BARRISUO RUIZ, *Administración electrónica…*, cit., 2007, p. 23; DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, p. 56; COTINO HUESO, "Derechos del ciudadano…", cit., 2008, p. 119, subraya que la Administración electrónica ha venido para quedarse

[90] TORNE-DOMBIDAU JIMENEZ y CASTILLO BLANCO, "Informática y Protección...", cit., 1993, p. 268.

[91] PIÑAR MAÑAS, "Nuevas tecnologías…", cit., 2008, p. 971; TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, pp. 568-569.

[92] COTINO HUESO, "Derechos del ciudadano…", cit., 2008, p. 120, hace referencia a las ventajas de la Administración electrónica para el ciudadano; GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración*…, cit., 2008, pp. 16-17.

[93] TORNE-DOMBIDAU JIMÉNEZ y CASTILLO BLANCO, "Informática y Protección...", cit., 1993, p. 268, evidencian cómo "es muy frecuente que el procedimiento administrativo requiera el intercambio de información entre distintos servicios para contrastar o completar los datos suministrados por los ciudadanos, lo que, en ausencia de una comunicación fluída y utilización adecuada de los medios informáticos, suele repercutir en el alargamiento de los trámites y tiempos de respuesta excesivos en la prestación de los servicios".

[94] INAP, *Libro Blanco sobre la Administración Electrónica y la Protección de Datos Personales,* Documentos INAP, nº 27, 2003, p. 55, resalta la necesidad de reeditar el pacto entre administración y usuario.

[95] VELÁZQUEZ BAUTISTA, *100 Interrog@antes...,* cit., 2004, p. 175.

[96] GARCÍA-POGGIO, "Hacia una...", cit., 1998, p. 8 explica estos tres instrumentos.

de forma más efectiva, sino que conlleva un cambio sustantivo, de fondo, estructural, de valores[97]. Este nuevo modelo de Administración supone que se incorporen las TIC a la misma y que el conjunto de órganos que la componen asuman una nueva filosofía en su funcionamiento, más flexible y ágil, que sitúa al ciudadano más en el centro que nunca[98].

La sociedad actual exige de la Administración una evolución. Como se ha dicho por la doctrina, "El grado de eficacia de una organización se mide por su grado de adaptación"[99]. En la medida en que la Administración incorpora las nuevas tecnologías a su funcionamiento y adecua su organización a la nueva situación se hacen efectivas unas posibilidades que antes eran impensables. No ya porque conlleva la realización más eficaz y eficiente de las funciones administrativas, sino porque abre nuevas puertas a la participación ciudadana en los asuntos públicos[100], lo que repercute en su legitimidad[101]. Siguiendo esta línea la propia jurisprudencia ha reconocido de manera expresa la conveniencia de adoptar todos los instrumentos necesarios, incluso personales, para hacer efectiva la Administración electrónica[102].

La verdadera revolución de la Administración electrónica, por lo tanto, la plantea el situar más que nunca al ciudadano en el centro de la organización[103]. La incorporación de las nuevas tecnologías al funcionamiento y organización de las administraciones no sólo conlleva que se mejoren los servicios que prestan a los ciudadanos, sino que ha de tener como resultado una mayor participación de las personas en los asuntos de interés general.

Hacer efectivo este proyecto no resulta sencillo, menos aún cuando se trata de transformar una organización tan compleja como la Administración. Las barreras a salvar son numerosas. Podrían enumerarse unas cuantas: falta de seguridad en el uso de las TIC; coste de las infraestructuras; falta de calidad de los contenidos en Internet; falta de adaptación ante el constante y rápido avance de las tecnologías; necesidad de formación; la inexistencia de suficiente extensión y penetración de las TIC y en particular de Internet en los hogares[104]; cultura incipiente del uso de Internet más allá de un elemento de información y publicidad; la

[97] GAMERO CASADO, "El derecho administrativo…", cit., 2008, pp. 34-35.
[98] CRIADO GRANDE y RAMILO ARAUJO, "eAdministración, ¿un reto...", cit., 2001, p. 14, "las TIC e internet (...) podrían ser un motor de cambio para las organizaciones (...). Motor para el cambio organizativo en las administraciones entendiendo como tal no sólo la modificación de los elementos técnicos (...) sino también, lo que es más importante: el cambio en los valores y comportamientos que configuran la cultura organizativa existente".
[99] NIETO, "Reforma Administrativa...", cit., 1989, p. 128.
[100] RÍOS INSUA, FERNÁNDEZ y MARÍA RÍOS, "Más allá...", cit., 2004, "Numerosos autores, hoy llamados tecnoutópicos, (...) ven en *Internet* un medio para propagar globalmente los ideales, mitificados en nuestra opinión, del ágora ateniense o del *towm meeting* inglés, por medio de la discusión y votación electrónica. Cualquier decisión podría votarse y podríamos vivir en un sistema de referendum permanente". Como ejemplo de esta posición pueden citarse unas palabras de MORRIS: "Cuando la democracia directa arraigue, el votante americano se hará más comprometido y activo. No tendremos que esperar más a las siguientes elecciones para expresar nuestra opinión mientrss el congreso toma las decisiones por nosotros. No tendremos que esperar una encuesta para decir lo que nos plazca. Vamos a tomar Internet y decir a nuestros representantes qué hacer siempre que nos dé la gana".
[101] JORDANA, "Las Administraciones...", cit., 1999, p. 17.
[102] STS 21 de enero de 2009, FJ 4.
[103] COTINO HUESO, "Derechos del ciudadano…", cit., 2008, p. 122.
[104] Sólo el 54% de los hogares españoles tiene acceso a Internet, según el Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y la SI) "La Sociedad en Red", 2009, http://www.ontsi.red.es.

desconfianza en los medios de intercambio electrónicos[105]; desconocimiento de la existencia de la e-Administración; no se ha trabajado en la integración de sistemas; ausencia de liderazgo institucional claro: se confunden proyectos, etc.; no existe orientación al cliente; el marco tecnológico avanza más rápido que el normativo[106]. La superación de estos obstáculos ha de fundarse, sobre todo, en planes o proyectos que tengan en cuenta todos los factores que inciden en el adecuado desarrollo de una eficaz, y utilizada, Administración electrónica.

II.2. ¿Existe un verdadero compromiso institucional para el cambio?

El reto de incorporar las TIC a la Administración para hacer efectiva la transición a la Administración electrónica ha sido aceptado por el legislador, si bien con un éxito cuestionable[107]. En la Ley de Procedimiento Administrativo de 1958 se hacían guiños a la modernización tecnológica de la Administración. Sin embargo, hasta la vigente LPAC no se ha realizado una apuesta seria por la informatización del aparato público. Lo dispuesto en la norma anterior no pasaba de ser una declaración ambigua de intenciones que no imponía obligación alguna[108]. En este sentido, la actual Ley supone un salto cualitativo de gran entidad[109], inevitable, por otro lado, debido al momento histórico en la que se sitúa. En primer lugar porque deja, aparentemente, a un lado las declaraciones ambiguas para realizar una apuesta en principio decidida por la informatización de la Administración, y, en segundo lugar, porque toma en consideración la necesidad de emplear las TIC en la relación con los ciudadanos y no sólo en el ámbito interno[110].

[105] La propia LAE, artículo 3.3, señala como una de sus principales finalidades la creación de las condiciones de confianza necesarias en el uso de los medios electrónicos.

[106] CRIADO GRANDE y RAMILO ARAUJO, "eAdministración, ¿un reto...", cit., 2001, p. 21; COTINO HUESO, "Derechos del ciudadano…", cit., 2008, p. 119, señala que todavía hoy los ciudadanos no interactúan con normalidad con la Administración electrónica. "España lidera la Administración electrónica, pero apenas se utiliza", *Público.es*, 28 septiembre de 2010, se hace referencia al Informe de 2009 del Observatorio Nacional de las Telecomunicaciones y la SI, en el que pone de manifiesto la falta de compromiso de los ciudadanos con el empleo de las TIC para realizar las tareas comunes ante las administraciones;. Según indica el Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y la SI) "La Sociedad en Red", 2009, http://www.ontsi.red.es, el empleo por parte de los ciudadanos de la Administración electrónica se limita al pago de impuestos y a la solicitud de documentos y certificados, mientras que los servicios de ventanilla única están en desuso.

[107] GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración*…, cit., 2008, pp. 15-16.

[108] Ley de Procedimiento Administrativo, 17 de julio de 1958: "*Se racionalizarán los trabajos burocráticos y se efectuarán por medio de máquinas adecuadas, con vista a implantar una progresiva mecanización y automatismo en las oficinas públicas, siempre que el volumen del trabajo haga económico el empleo de estos procedimientos*".

[109] DE ASÍS ROIG, "Documentos Electrónicos...", cit., 1996, p. 146, afirma que la LPAC "manifiesta una inequívoca opción por un proceso generalizado de incorporación de estos medios a la administración"; OCHOA MONZÓ, "¿Hacia la ciberadministración...", cit., 2000, p. 156, subraya la intención de la LPAC de "dar carta de naturaleza a la incorporación de las técnicas informáticas y telemáticas en la relación ciudadano-administración".

[110] Exposición de Motivos LPAC: "Las nuevas corrientes de la ciencia de la organización aportan un enfoque adicional en cuanto a mecanismos para garantizar la calidad y transparencia de la actuación administrativa, que configuran diferencias sustanciales entre los escenarios de 1958 y 1992. La Ley de Procedimiento Administrativo de 1958 pretendió modernizar las arcaicas maneras de la Administración española, propugnando una racionalización de los trabajos burocráticos y el empleo de <<máquinas adecuadas, con vista a implantar una progresiva mecanización y automatismo en las oficinas públicas, siempre que el volumen de trabajo haga económico el ampleo de estos procedimientos>>. Este planteamiento tan limitado ha dificultado el que la informatización, soporte y tejido nervioso de las relaciones sociales y económicas de nuestra época, haya tenido hasta ahora incidencia sustantiva en el procedimiento administrativo, por falta de reconocimiento formal de la validez de documentos y comunicaciones emitidos por dicha vía. El extraordinario avance experimentado en nuestras Administraciones Públicas en la tecnificación de sus medios operativos, a través de su cada vez mayor parque informático y telemático, se ha limitado

Según reza la Exposición de Motivos de la LPAC "las técnicas burocráticas formalistas, supuestamente garantistas, han caducado, por más que a algunos les parezcan inamovibles, y la Ley se abre decididamente a la tecnificación y modernización de la actuación administrativa en su vertiente de producción jurídica y a la adaptación permanente al ritmo de las innovaciones tecnológicas". No obstante lo desafortunado de este pronunciamiento[111], la intención que se vislumbra en el fondo es clara[112]. Se trata de sustituir el elemento humano o el elemento papel por el elemento ordenador[113]. Consiste, en definitiva, en sacarle todo el partido posible a la telemática.

Esta voluntad se concreta en el artículo 45 de la LPAC: "*Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias*"[114]. El vigor y la determinación con la que se pronunciaba el legislador en la Exposición de Motivos parece rebajarse en esta disposición en la que las administraciones públicas simplemente se ven obligadas a "impulsar" la aplicación de las nuevas tecnologías. Lo cierto es que se deja en esta norma un amplio margen de actuación a las entidades públicas para la incorporación de las nuevas tecnologías, lo que se contrapone con la posición tan firme y decidida que el legislador adopta en la Exposición de Motivos[115]. Además de en el citado precepto, en el artículo 38.3 de la norma parece hacerse una apuesta definitiva por la integración de las TIC obligando a la Administración a implantar los registros en soporte informático[116]. Sin embargo, también en este caso la informatización se hará depender del grado de desarrollo de los medios técnicos disponibles por las diversas Administraciones[117].

A pesar de la ambigüedad que se desprende de la letra de los citados preceptos la doctrina ha entendido que de una lectura sistemática de todo el ordenamiento puede deducirse una clara obligación de la Administrasción de adaptarse a la nueva realidad social. En concreto se ha interpretado que el principio constitucional de eficacia, que informa toda la actividad administrativa, obliga al aparato público a adoptar todas las medidas necesarias para adaptar su funcionamiento a la realidad social existente[118].

---

al funcionamiento interno, sin correspondencia relevante con la producción jurídica de su actividad relacionada con los ciudadanos".

[111] No hay que olvidar que las exigencias formales de los procedimientos administrativos constituyen, cuando menos en parte, verdaderas garantías para los ciudadanos.

[112] AGIRREAZKUENAGA y CHINCHILLA, "El Uso...", cit., 2001, p.39, opinan que del apartado 5 de la Exposición de Motivos rezuma un "absurdo entusiasmo".

[113] FROSINI, "Informática y Administración...", cit., 1994, p. 453, habla de "la transformación de la Administración Pública tradicional (basada en el binomio hombre-papel) hasta la nueva fase de la administración automatizada, en la que el ordenador sustituye (aunque parcialmente) ya sea el elemento humano, efectuando directamente los cálculos y las comparaciones exigidas por un acto administrativo, así como el elemento papel".

[114] Artículo 45.1 LPAC.

[115] DAVARA RODRÍGUEZ, *Acceso electrónico…*, cit., 2010, p. 9, pone de manifiesto que la letra del artículo 45 LPAC no representaba más que una cuestión de buena voluntad.

[116] Artículo 38.3 LPAC: "*Los registros generales, así como todos los registros que las Administraciones públicas establezcan para la recepción de escritos y comunicaciones de los particulares o de órganos administrativos, deberán instalarse en soporte informático.(...)".*

[117] Disposición Adicional 2 LPAC.

[118] VALERO TORRIJOS, *El Régimen...*, cit., 2004, p. 9.

Hoy día, más allá de los problemas interpretativos que se pudieran deducir de la redacción de la LPAC es indiscutible que esta realidad se está construyendo a golpe de ordenador. Así lo han entendido también los poderes públicos. Las últimas normas aprobadas en relación a esta cuestión reflejan el indudable compromiso de adaptar, de mejor o peor manera, la Administración a las actuales exigencias. El preámbulo del RD 209/2003 de 21 de febrero, por el que se regulan los Registros y las Notificaciones Telemáticas, así como la Utilización de Medios Telemáticos para la Sustitución de la Aportación de Certificados por los Ciudadanos señala que "*Una de las ideas subyacentes a este Real Decreto es el fomento de una nueva cultura administrativa en la que el papel, en la medida de lo posible vaya siendo sustituido por los documentos telemáticos*". Por su parte, la LAE constituye en sí misma reflejo del citado compromiso, al reconocer expresamente el derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos[119] y la obligación de las administraciones de utilizar las tecnologías de la información[120]. Parece, como afirma algún autor, que "la Administración ha comenzado a leer a NICHOLAS NEGROPONTE"[121] y que el objetivo que se marcaba en la Exposición de Motivos de la LPAC empieza a tornarse en un reto importante. Tanto, que a día de hoy la mayoría de indicadores sitúan al Estado en posiciones adelantadas a nivel mundial en lo que concierne a la Administración electrónica[122].

Más allá de lo que dicten las leyes, dependerá de la voluntad política el que la Administración Electrónica pase a ser una realidad en un futuro cercano[123]. Hacer efectivas las citadas previsiones normativas depende, en gran parte, de las iniciativas que se adopten. A nivel europeo, el "Plan e-Europa, una Sociedad de la Información para todos" reconoce la trascendencia de incorporar las TIC a las distintas administraciones, subrayando la necesidad de implantar estas nuevas tecnologías para posibilitar un intercambio fluido de información entre los diferentes entes públicos en el marco de la Unión, que a su vez favorecerá la movilidad de los ciudadanos. Esta necesidad se ha plasmado, por ejemplo, en el denominado Plan IDA (Interchange of Data between Administrations)[124]. En la actualidad, en el ámbito de la UE el plan de acción sobre administración electrónica i2010 se dirige a hacer más eficaces los servicios públicos, a modernizarlos y a ajustarlos a las necesidades de la población. Para ello, plantea como objetivos prioritarios la implantación de la administración electrónica para todos, hacer una Administración más eficaz reduciendo la carga administrativa, integrar elementos técnicos suficientes y fomentar la participación ciudadana en los asuntos públicos[125].

[119] Artículo 6, LAE. GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración*…, cit., 2008, p. 28; COTINO HUESO, "Derechos del ciudadano…", cit., 2008, p. 167 y siguientes; VELEIRO, *Protección de Datos…,* cit., 2008, p. 349.

[120] Artículo 2, LAE. DAVARA RODRÍGUEZ, *Acceso electrónico…,* cit., 2010, p. 11, subraya la importancia de la LAE en la medida en que pasa de fijar una mera declaración de voluntad a una obligación para las administraciones.

[121] COBEÑA FERNÁNDEZ, "Evolución de los sistemas...", cit., 1998.

[122] Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y de la SI), "La Sociedad en Red 2009", http://www.ontsi.red.es.

[123] MARTIN COBISA, "Las Nuevas...", cit., 1998, p. 106

[124] http://europ.eu.int/scadplus/leg/en/lbv/124147a.htm

[125] Comunicación de la Comisión, 25 de abril de 2006, "Plan de acción sobre administración electrónica i2010: acelerar la administración electrónica en Europa en beneficio de todos". BARRIUSO RUIZ, *Administración electrónica…,* cit., 2007, pp. 24-27.

A nivel estatal cabe destacar el "Plan de Choque para el impulso de la Administración Electrónica en España"[126], de 8 de mayo del 2003, que recogía sistemáticamente los principales ejes sobre los que la Administración tiene que actuar para evolucionar hacia una Administración Electrónica plena. Así, facilitar el acceso público a los usuarios, impulsar el desarrollo de servicios para los usuarios, facilitar el intercambio de información entre administraciones públicas, y apoyar la reorganización interna de procesos en las administraciones públicas constituyen las líneas maestras sobre las que hay que actuar. El objetivo era lograr una Administración más cercana al ciudadano, más abierta, y más eficaz. En octubre de 2004 se aprobó un nuevo plan para la transformación de la Administración. Se trataba del Plan Conecta[127], que contaba con cinco pautas principales de actuación: CERTIFICA, para el desarrollo de sistemas de interacción de datos entre las Administraciones Públicas y el ciudadano, con el objetivo principal de sustituir los certificados en papel por certificados por *Internet* con validez jurídica; eDNI: DNI electrónico que sustituya al actual y que permita a los ciudadanos identificarse y firmar en el mundo telemático; CIUDADANO.es, para acercar la Administración al ciudadano; SIMPLIFICA, que busca una gestión pública racional y eficiente; y MAP.es, que tratará de actualizar y mejorar tecnológicamente el MAP. Hoy día, tras la aprobación de la LAE, los diferentes proyectos vinculados al desarrollo de la Administración electrónica se dirigen a la concreción de los aspectos arriba citados dentro del plan avanza 2, que, sin embargo, hace un especial énfasis en el apoyo a las entidades locales y en el desarrollo del DNI electrónico[128].

En el ámbito autonómico, en el Plan Euskadi en la Sociedad de la Información "Agenda digital de Euskadi" 2010, la Administración electrónica constituye una prioridad. Este plan recoge acciones en una doble dirección. Primero, desde una perspectiva interna, pretende dotar a la Administración de la plantaforma necesaria para hacer efectiva la Administración electrónica. Y segundo, trata de incidir en una serie de puntos que afectan a la relación de la Administración con los ciudadanos: el fomento de la participación ciudadana y una Administración interconectada, integrada, eficiente y de calidad son los objetivos principales. De una manera más concreta el Plan Estratégico de Administración y Gobierno Electrónico 2008-2010, reclama las mismas actuaciones, basándose en cuatro ejes: digitalización, Gobierno a disposición de la cuidadanía, nueva organización y cultura de trabajo y colaboración con otras administraciones[129].

II.3. La eAdministración y el riesgo de control social.

Una vez las potencialidades de la Administración electrónica se hayan desarrollado y el uso de todos los servicios que propone se generalice, el flujo de información vinculada a los ciudadanos será una constante en la práctica administrativa. Si ya en tiempos precedentes la Administración constituía un caudal importante de información sobre los ciudadanos, como antes lo fuera la iglesia, ahora, con las posibilidades que otorgan las nuevas tecnologías, el aparato público puede convertirse en el "ojo que todo lo sabe". Las TIC dan una gran oportunidad para

[126] http://www.igsap.map.es/ticker/does/plan_choque.pdf/
[127] http://www.map.es/.
[128] VELEIRO, *Protección de Datos…,* cit., 2008, p. 357 y siguientes, donde analiza la Administración electrónica desde la perspectiva del Plan Avanza.
[129] Plan estratégico de Administración y Gobierno Electrónicos 2008-2010.

alcanzar una administración cercana, accesible, eficaz y transparente, pero, empleadas de forma irregular, las nuevas tecnologías pueden convertirse en un aliado perverso del poder[130].

En un Estado social en el que los poderes públicos se obligan a prestar una serie de servicios, la Administración debe hacerse con una ingente cantidad de datos de carácter personal para poder cumplir sus funciones[131]. Piénsese en ejemplos tan cotidianos como la Hacienda Pública o la sanidad. De esta manera, la Administración se convierte en un ente con una gran cantidad de ficheros con información referida a los ciudadanos. Primero, por ser fuente de información que genera sobre sí misma, y segundo, por ser receptora de información que le llega desde los propios ciudadanos[132].

Para poder manipular todos estos datos y cumplir así con su función constitucional, que no es otra que la de satisfacer el interés general, son necesarios unos sistemas de información muy avanzados que posibiliten la manipulación de la información con rapidez y seguridad. Pues bien, las TIC ofrecen esa posibilidad[133].

En principio, la manipulación de información empleando las nuevas tecnologías por parte de los poderes públicos se dirige a la realización de la actividad administrativa, fundamentalmente la prestación de servicios públicos. Sin embargo, se abraza aquí la siguiente afirmación: "la gran eclosión de las lesiones a la esfera personal de los sujetos por lo que respecta al tratamiento de sus datos personales encuentra en gran medida su origen en el desarrollo de un modelo de Estado que ha nacido precisamente para proteger al individuo y para garantizar las más óptimas condiciones para su desarrollo personal y colectivo y la defensa de sus derechos inalienables"[134].

El propio Estado puede convertirse en agresor. El uso ilegítimo de las nuevas tecnologías no puede venir sólo de piratas informáticos o ciberdelincuentes, sino también del aparato público. Es un hecho ya contrastado la existencia de sistemas de interceptación de comunicaciones como ECHELON o Carnivore, que son empleados por los Estados, a veces respaldados por una normativa cada vez más restrictiva con los Derechos Humanos, y a veces de forma contraria al marco jurídico existente[135]. En el ámbito estatal este debate se ha generado en relación al conocido caso del empleo por parte de la Administración del sistema SITEL (Sistema Integral de Interceptación de Comunicaciones Electrónicas). Se ha planteado ante los tribunales la duda sobre si el sistema empleado en el Estado para la interceptación de comunicaciones es acorde a

[130] PIÑAR MAÑAS, "Nuevas tecnologías…", cit., 2008, p. 967.
[131] TONIATTI, "Libertad Informática...", cit., 1991, p. 141; REESE, KUBICEK, LANGE, LUTTERBECK, y REESE, *El impacto*..., cit., 1982, p. 100, que "en este tipo de sistema sólo recibe ayuda del Estado el ciudadano que está dispuesto a demostrar su derecho a cualquier prestación a base de poner a disposición de éste todos sus datos personales".
[132] SOUVIRÓN, "En torno...", cit., 1994, p. 121.
[133] OROZCO PARDO, "Los Derechos...", cit., 1994, p. 152, afirma que "sería la "Razón de Estado" como fundamento del conocimiento de datos".
[134] FERNÁNDEZ SALMERÓN, *La Protección...*, cit., 2003, p. 85; GÓMEZ NAVAJAS, *La Protección*..., cit., 2005, pp. 34-35.
[135] MAGRO SERVET, "La delincuencia informática…", cit., 2004; PÉREZ LUÑO, "Derecho y nuevas tecnologías…", cit., 2005, pp. 234-235; GUERRERO PICÓ, *El Impacto de Internet*..., cit., 2006, p. 344.

Derecho y respeta la intimidad de las personas[136]. A lo largo de este trabajo se irán viendo diferentes supuestos en que las admnistraciones, en este caso sanitarias, han sido sancionadas por incumplir la normativa de protección de datos.

Las administraciones públicas siempre han empleado datos de carácter personal. Sin embargo, a partir del fatal acontecimiento sucedido el 11 de septiembre de 2001 en Nueva York la lucha contra el terrorismo y la búsqueda de la seguridad han dado lugar al empleo de técnicas que directamente atentan contra Derechos Fundamentales como la intimidad y la autodeterminación informativa[137]. El uso de mecanismos de intromisión en la vida privada de los individuos se ha convertido en un arma fundamental en la lucha por la seguridad. Así, la búsqueda del equilibrio entre intimidad/autodeterminación informativa y seguridad se constituirá en uno de los retos principales a perseguir por organizaciones defensoras de los Derechos Humanos y Gobiernos del mundo del presente[138]. Desde el TEDH se ha puesto de manifiesto en numerosas ocasiones la necesidad de encontrar el equilibrio entre la conveniencia de emplear las nuevas tecnologías con fines de investigación criminal y el derecho a la vida privada. Es lo que ha sucedido, por ejemplo, cuando determinadas administraciones han pretendido conservar información, extraída empleando nuevos intrumentos, vinculada a personas acusadas pero no condenadas, de haber cometido un delito. Ha señalado el tribunal que si bien es cierto que con las nuevas tecnologías pueden extraerse informaciones de gran utilidad, incluso vinculadas al ADN, éstas no pueden ser empleadas ni almacenadas indiscriminadamente[139]. En sentido similar cabe destacar la reciente sentencia del Tribunal Consitucional Federal de Alemania, que ha decretado la inconstitucionalidad de determinados preceptos de la Ley Federal de Telecomunicaciones y del Código Procesal Penal, por entender que vulneran el derecho al secreto de las comunicaciones y el derecho a la autodeterminación informativa[140]. Estas normas obligaban a los proveedores de servicios de telecomunicaciones a almacenar masivamente los datos vinculados a las comunicaciones por teléfono, correo electrónico, fax, Internet, etc, para poder ser empleados por las autoridades en la persecución de infracciones. Considera el tribunal que una tal regulación sólo puede considerarse acorde a Derecho en caso de que respete los principios de proporcionalidad y transparencia, y posibilite el uso de esos datos únicamente en

[136] SSTS 2 de febrero de 2008 y 30 de diciembre de 2009. "Sitel permite escuchar a miles de investigados por delitos graves", *Público.es,* 6 de noviembre de 2009. MARTÍNEZ FERRÍZ, "La operatividad de SITEL…", cit., 2010; MARTÍN PALLÍN, "Intimidad, privacidad…", cit., 2010, p. 1.336 y siguientes.

[137] PIÑAR MAÑAS, "Protección de Datos…", cit., 2009, p. 148.

[138] SÁNCHEZ BRAVO, "El Control..*."*, cit., 2002, y FERNÁNDEZ CHATEIGNER, "La Protección...", cit., 2003. MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, pp. 44-50, señala la necesidad de que las Fuerzas y Cuerpos de Seguridad empleen las nuevas tecnologías con responsabilidad. 29ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, en Montreal, del 26 al 28 de septiembre de 2007. Resolución sobre la necesidad urgente de normas internacionales para proteger los datos de pasajeros que usarán los gobiernos a los efectos de la aplicación de la ley y la seguridad en las fronteras: *"*La Conferencia observa que: -los gobiernos solicitan de manera creciente datos sobre los pasajeros para usarlos en la lucha contra el terrorismo, la inmigración ilegal y otros delitos sin suficiente consideración por los derechos humanos y de privacidad de los pasajeros; -Algunos datos sobre pasajeros pueden usarse para hacer inferencias sobre religión, origen étnico y otros aspectos sumamente delicados". "El carácter de los viajes internacionales es tal que se necesita un enfoque global y se requiere una solución global urgente a fin de asegurar niveles apropiados de seguridad e inspirar confianza en los pasajeros, proporcionando al mismo tiempo medidas apropiadas que incluyan las necesarias salvaguardias de protección de los datos y la privacidad".

[139] STEDH 4 de diciembre de 2008, S. y Marper v. Reino Unido, FFJJ 105 y siguientes.

[140] STC Federal Alemán 2 de marzo de 2010, 11/2010.

determinados casos, para la investigación de determinados crímenes y en condiciones de seguridad en el tratamiento de la información. Es decir, no puede permitirse un uso indiscriminado y generalizado de esta información, a pesar de que se lleve a cabo por la propia Administración y para llevar a cabo fines como la persecución de infracciones, pues lo contrario llevaría a que fuera posible la creación, por parte de los poderes públicos, empleando dichos datos, de perfiles completos de todos los ciudadanos.

Lo cierto es que las TIC pueden configurarse en manos de un cuerpo tan poderoso como la Administración, como un instrumento de control social de alcance hasta ahora desconocido[141]. Técnicas que siempre se han relacionado con regímenes totalitarios se emplean en Estados considerados democráticos y que, sobre todo a partir de 1948, se constituyeron en defensores y promotores de los Derechos Humanos[142], creando una gran situación de desconfianza entre los ciudadanos y la sensación de estar viviendo en una vitrina, lo que se ha denominado el "síndrome del pez rojo"[143]. Uno de los últimos ejemplos de que los estados democráticos pueden llevar a cabo actuaciones que colocan al ciudadano ante esa situación de sentirse vigilado lo constituye el acuerdo entre la UE y los EEUU para transmitir datos bancarios en el ámbito de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT), con el fin de combatir el terrorismo. Tras una intensa polémica al respecto, el Parlamento europeo ha acordado con las autoridades norteamericanas la posibilidad de que estas últimas accedan a determinados dados de contenido económico con el citado objetivo[144].

Las TIC en manos de la Administración Pública pueden constituir un instrumento realmente positivo o todo lo contrario, un mecanismo de control social sin precedentes[145]. El que no se opte por el segundo camino y se llegue a una situación cercana de la descrita por Orwell en su "1984", depende de que se configure una normativa que garantice la integridad y respeto de los derechos fundamentales.

III. LAS TIC EN EL ÁMBITO SANITARIO.

Cuando se dice que las TIC se han incorporado prácticamente a todos los ámbitos en los que se desarrolla la vida, sobra decir que los centros sanitarios no han constituido una excepción. Aunque la integración de la telemática en los hospitales está resultando más lenta que en otros campos, ya se aplican proyectos concretos dirigidos a manipular la información en este entorno.

---

[141] REBOLLO DELGADO, *Derechos Fundamentales…*, cit., 2004, p. 66. Un ejemplo cercano de lo dicho podría ser la posibilidad a la que se refiere el Dictamen APDCat. CNS 47/2009, de que los interventores de un Ayuntamiento puedan conocer a través de las facturas y otras indagaciones el núermo al que llaman los trabajadores de la administración e incluso el motivo de las llamadas, con el fin de controlar el gasto producido por el uso de los teléfonos.

[142] FERNÁNDEZ CHATEIGNER, "La Protección...", cit., 2003, p. 5, y FERNÁNDEZ SALMERÓN, *La Protección...*, cit., 2003, pp. 86-87.

[143] PÉREZ LUÑO, *Manual de Informática...,* cit., 1996, p. 85: "La Administración Publica aparece como un organismo de poderes mucho más sutiles e inaplacables que los imaginados por Hobbes en su Leviathan".

[144] Decisión del Consejo Europeo, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo, 24 de junio de 2010.

[145] PIÑAR MAÑAS, "Nuevas tecnologías…", cit., 2008, p. 980; MARTÍN PALLÍN, "Intimidad, privacidad…", cit., 2010, p. 1.332.

III.1.La información: elemento básico de la práctica sanitaria.

La actividad administrativa se basa, en gran parte, en el tratamiento de la información. En la práctica sanitaria la manipulación de datos constituye una actividad fundamental, si no la más importante. Todo tratamiento médico tiene que partir necesariamente de una información veraz, completa y actual sobre el paciente. Desde que se nace, e incluso desde antes de nacer, hasta la muerte, e incluso después de ésta, las personas son fuente constante de información en el sector sanitario[146]. Esta información resulta imprescindible para la realización de las tareas vinculadas a la protección de la salud.

En el ejercicio de la medicina la práctica totalidad de funciones están relacionadas de alguna manera con la información[147]. La actividad puramente asistencial, la investigadora, la actividad estrictamente administrativa o gestora, la estadística, etc., requieren de la manipulación de datos relacionados a personas identificadas o identificables. Se puede afirmar que el sanitario, es uno de los sectores en que la información adquiere mayor trascendencia[148].

Este hecho no constituye por sí mismo ninguna novedad. La importancia de la información en este ámbito siempre ha sido especialmente destacable. Lo verdaderamente reseñable en la actualidad es que se ha puesto más que nunca de manifiesto la dificultad de los sistemas sanitarios para manipular esta información. Cada vez son más los servicios que se prestan desde los centros sanitarios, la población envejece cada vez más, la movilidad de los ciudadanos aumenta, aparecen nuevas fuentes de información como la genética, la especialización es también cada vez mayor, a la información sanitaria hay que sumarle la administrativa, etc. Todo esto hace que la gestión sanitaria en general y la manipulación de la información sanitaria en particular, constituyan actividades cada vez más complejas.

El volumen de datos que hay que manipular y la agilidad con la que hay que hacerlo para otorgar un servicio de calidad hacen que sean prácticamente imprescindibles herramientas que posibiliten este tratamiento fácil, rápido y seguro de la información sanitaria[149], un "sistema de información"[150] que ponga a disposición del personal que lo necesite la información que sea precisa para llevar a cabo su labor, cuando y como lo requiera. La implantación de un sistema de

[146] Instrucción 1/2009, 17 de diciembre de 2009, sobre el tratamiento de datos personales de los recién nacidos en los centros asistenciales que integran la red sanitaria única de utilización de la Comunidad de Madrid.
[147] MARIMÓN, *La Sanidad...*, cit., 1999, p. 43: "El porcentaje de actividad relacionada con la información se acerca (...) al 100%", "si valoramos la importancia de los componentes básicos utilizados, diferenciando los físicos (o químicos), esto es, materia y energía, de los informativos, vemos que sólo en los servicios generales (mantenimiento, almacenes, cocina lavandería) predomina claramente la componente física".
[148] HIGH LEVEL COMMITTE ON HEALTH, *Health Telematics Working Group of the High Level Committe on Health: Final Report*, 01/04/03, http://www.eu.ent/: "*Information is a vital resource for the effective running of all mayor businesses (...). The health sector is arguably one of the most information dependent businesses of all*".
[149] ALONSO LÓPEZ (Coordinador), *Informatización en...*, cit., en http://www.semfyc.es/; DE MIGUEL SÁNCHEZ, *Secreto médico…,* cit., 2002, p. 260.
[150] GARCÍA GÓMEZ, "Sistema de Información...", cit., 2003, "entendido (sistema de información) como la organización compuesta por personal, material y métodos para recoger, procesar, analizar y transmitir la información necesaria para apoyar la formulación, desarrollo, segimiento y evaluación de las políticas de salud".

información capaz de responder a las necesidades actuales de transmisión y manejo (acceso, actualización etc.) de datos pasa por la informatización del sistema[151].

La implantación de las nuevas tecnologías en el sector sanitario resulta un proceso inevitable. Este proceso, sin embargo, no se debe considerar como un fin en sí mismo, sino como un instrumento cuyo fin se dirige a prestar un mejor servicio sanitario, que es el objetivo de las TIC aplicadas a la sanidad. Y hay que subrayar este punto porque esto no siempre ha sido así[152]. En ocasiones, las necesidades de los médicos, de la estructura de los centros, o de las marcas comerciales se han superpuesto a los intereses de los pacientes y de la sociedad en general. Sea como sea, parece evidente que en la actualidad la incorporación de las nuevas tecnologías al ámbito sanitario ha creado nuevos entornos o realidades que merecen una particular atención. Es el caso de la telemedicina[153].

III.2. Aspectos generales de la telemedicina.

Antes de pasar a analizar proyectos concretos de TIC aplicadas al ámbito sanitario, merece la pena detenerse brevemente en el estudio de algunos aspectos generales de la incorporación de las nuevas tecnologías a este entorno.

III.2.1.Definición[154]

El concepto de "telemedicina" se ha entendido de muy distintas formas por diferentes sectores de la doctrina. En un sentido estricto, eminentemente literal, se ha interpretado que la "telemedicina" es la práctica de la medicina a distancia[155]. Se trata de la definición admitida por la mayoría[156]. Esta acepción encuentra fundamento en los antecedentes históricos que se han vinculado a la telemedicina. Las distintas experiencias que se relacionan con la telemedicina moderna, que emplea la telegrafía, telefonía, radio, TV y medios inalámbricos como satélites y teléfonos móviles para llevar a cabo la transmisión de informaciones[157], se refieren a la práctica de la medicina a distiancia. El estetoteléfomo, que aparece a finales del s. XIX, la telecardiología, que nace a inicios del s. XX, son claro ejemplo. Lo mismo ocurre con la tan conocida portada del nº de abril de 1924 de la revista *Radio News,* que presentaba una idea visionaria de la telemedicina en la que se planteaba la posibilidad de transmitir una imagen a distancia[158], o la primera demostración de telemedicina entre varios Estados que se da en 1951 en la Feria Mundial de New York[159]. En la que se ha llamado "la segunda era de la telemedicina", que se

[151] CUSTODI y GARCÍA, "Los Sistemas...", cit., 2002; MÉJICA GARCÍA, *El Enfermo Transparente…*, cit., 2002, p. 15.
[152] ALONSO LÓPEZ y GANCEDO GONZÁLEZ, "Informatización integral...", cit., 1999, p. 282
[153] DE MIGUEL SÁNCHEZ, *Tratamiento de Datos…,* cit., 2004, p. 44.
[154] SÁNCHEZ-CARO y ABELLÁN, *Telemedicina y Protección...*, cit., 2002, pp.1-6, dan una completa visión de la evolución del concepto "telemedicina".
[155] FERRER ROCA, *La telemedicina...*, cit., 2001, p. 21, subraya el hecho de que la telemedicina sigue siendo "medicina", un servicio al ciudadano que tiene como rasgo sustancial que se practica a distancia.
[156] JACQUEMIN, "La Telemedicina...", cit., 2003.
[157] En http://www.mundoredondo1.com/ se da una visión global de las aplicaciones que estos medios han tenido en la medicina a lo largo de la Historia.
[158] DEL POZO GUERRERO y GÓMEZ AGUILERA, "Telemedicina: una visión...", cit., 2001, p. 445.
[159] SÁNCHEZ CARO y ABELLÁN, *Telemedicina y Protección...*, cit., 2002, p. 1.

produce a partir de los 90 y se relaciona, sobre todo, con la integración de elementos informáticos[160], ocurre lo mismo. En todos los casos la telemedicina se refería principalmente a la posibilidad de llevar a cabo la práctica asistencial a distancia.

Esta línea interpretativa parece haber tenido eco también en las definiciones que, tanto la Organización Mundial de la Salud (OMC), como la Asociación Médica Mundial (AMM) han dado de este concepto. La segunda entiende que la "telemedicina es la práctica de la medicina a distancia gracias a la cual las intervenciones, el diagnóstico, las recomendaciones y las decisiones terapeúticas se fundamentan en los datos clínicos, documentos y otras informaciones transmitidas por los sistemas de comunicación"[161]. Por su parte, la OMS la considera "el suministro de servicios de atención primaria, en los que la distancia constituye un factor crítico, por profesionales que apelan a las tecnologías de la información y la comunicación con objeto de intercambiar datos para hacer diagnósticos, preconizar tratamientos y prevenir enfermedades y heridas, así como para la formación permanente de los profesionales de atención a la salud y en actividades de investigación y evaluación, con el fin de mejorar la salud de las personas y de las comunidades en que viven"[162].

Esta acepción en la que se subraya la distancia como factor característico ha sido aceptada por numerosas instituciones[163]. Parece hacer referencia a una de las aplicaciones que tienen las TIC en el entorno sanitario, en concreto, a los casos en los que los pacientes se encuentran en lugares inaccesibles o no puedan desplazarse. Las definiciones aportadas por las citadas organizaciones pueden interpretarse, sin embargo, de otra manera. Se puede vislumbrar un concepto más amplio que el expuesto, donde lo realmente relevante no es que el paciente se encuentre lejos, sino el hecho de que se empleen las TIC para la práctica de la medicina. Evidentemente, la distancia, o más bien la relativización de este factor, es un elemento característico de las TIC, pues uno de los principales logros de las nuevas tecnologías consiste en burlar este límite. No obstante, cuando se hace referencia a la telemedicina no se quiere acentuar sólo este aspecto de las TIC, sino algo mucho más amplio.

Partiendo de esta idea algunos autores han puesto de manifiesto, se entiende aquí que acertadamente, la necesidad de dejar atrás el concepto tradicional de telemedicina para dar paso a una acepción más amplia. Se interpreta que la telemedicina es una nueva forma de proteger la salud de las personas en la que las nuevas tecnologías se erigen en instrumento fundamental

[160] MARTÍN SÁNCHEZ, "La congruencia...", cit., 2002, pp. 25-31.
[161] Preámbulo de la "Toma de Posición de la Asociación Médica Mundial sobre las Responsabilidades y Directrices Éticas ligadas a la Práctica de la Telemedicina", adoptada por la 51ª asamblea, celebrada en Tel Aviv, octubre 1999, http://www.wma.net/e/.
[162] SÁNCHEZ-CARO y ABELLÁN, *Telemedicina y Protección...*, cit., 2002, p.1.
[163] La *Ethical Guidelines in Telemedicine* adoptada por el Comité Permanente de Médicos Europeos, de abril de 1997, entiende que el término telemedicina "*refers to the practice of medicine over a distance. In telemedicine, interventions, diagnostic and treatment decisions and recomendations are based on data, documents and other information transmitted through telecommunication systems*".

para la consecución del fin. Se trata del uso de las TIC para salvaguardar la salud de las personas[164].

Así, se entiende la telemedicina en un sentido amplio, como una nueva forma de realizar la actividad sanitaria en la que lo característico es la aplicación de las TIC en todas las áreas de la actuación sanitaria: asistencial, de gestión, de investigación, de formación, entre otras. En este sentido se interpretaría como sinónimo de lo que se ha llamado "eSalud"[165], que ha sido definida como "*the application of ICT accross the whole range of functions that affect health*"[166].

III.2.2. Iniciativas políticas en torno a la telemedicina

El interés por el desarrollo de la telemedicina no se ha visto reflejado sólo en el ámbito científico, sino también en la esfera política, en los distinto proyectos que tratan de impulsar la sociedad de la información. En el ámbito europeo el Plan eEurope 2002 Una Sociedad de la Información para todos, dentro de su tercer objetivo "Estimular el uso de Internet", recogía la sanidad en línea como uno de los principales focos de actuación, asumiendo como reto el desarrollar una infraestructura de sistemas validados, interoperables y de fácil uso para la educación sanitaria, la prevención de las enfermedades y la asistencia médica. Con este objetivo planteaba 4 acciones, a saber: conseguir que los que prestan servicios sanitarios primarios y secundarios dispongan de una infraestructura telemática sanitaria, incluidas las redes regionales; detección y difusión de las mejores prácticas sobre servicios sanitarios por vía electrónica en Europa y establecimiento de criterios de evaluación comparativa; establecimiento de un conjunto de criterios de calidad para sitios *web* relacionados con la sanidad; y establecimiento de redes de evaluación de datos y tecnología sanitaria.

En la valoración que la Comisión realizó sobre la evolución del Plan eEurope 2002 en la Comunicación de la Comisión al Consejo al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, se valoraba positivamente lo logrado hasta entonces: un 78% de los médicos de la UE estaban conectados a Internet (48% en España); el 48% de ellos utilizaba archivos sanitarios electrónicos; el 46% utilizaba Internet para transmitir datos de los pacientes a otros profesionales, etc. Sin embargo, el mismo informe apuntaba que quedaba mucho por hacer, subrayando 6 criterios que había que tener en cuenta a la hora de aplicar las TIC en la actividad sanitaria: transparencia y veracidad, autoridad, protección de datos e intimidad, actualización de la información, fiabilidad y accesibilidad.

[164] DEL POZO GUERRERO y GÓMEZ AGUILERA, "Telemedicina: una visión...", cit., 2001, p. 448. La telemedicina es "una manera de calificar la forma de hacer y organizar los servicios para cuidar y restituir la salud de todos, e identifique el objetivo último de las tecnologías de la información y las comunicaciones en salud: facilitar la inmersión eficiente del sistema sanitario en el nuevo espacio electrónico de la SI". ROIG y SAIGI, "Dificultades para incorporar…", cit., 2009, "la telemedicina, definida como la utilización de las tecnologías de la información y la comunicación para la transferencia de información médica con finalidades diagnósticas, terapéuticas y educativas".

[165] WILSON, LEITNER and MOUSSALLI, *Mapping the potential...,* cit., 2004: Concepto que aparece entre 1999 y el año 2000.

[166] SILBER, *The case for eHealth...,* cit., 2003, se refiere a "la aplicación de las TIC a todo tipo de funciones que afectan a la protección de la salud".

El Plan eEurope 2005 seguía la línea marcada por el anterior plan en la labor de implantar la *eHealth*, sin embargo recogía proyectos concretos sobre los que actuar: Tarjeta Sanitaria Electrónica, Redes de Información Sanitaria y Servicios Sanitarios en línea, entre otros. En el marco de este plan, el 22-23 de mayo de 2003 se celebró la "*eHealth 2003 Conference*"[167]. En el seno de esta Conferencia se adoptó la "*Ministerial declaration on eHealth*" en la que ministros de los Estado que componen la UE, así como los asociados, los que van a tener acceso a la UE, y la EFTA adquirieron el compromiso de trabajar juntos para elaborar las mejores prácticas de las TIC como herramientas para mejorar la promoción y protección de la salud, así como la calidad, accesibilidad y eficiencia en todos los aspectos de la asistencia sanitaria[168]. Los principales compromisos adoptados en esta Declaración eran promover la calidad y mejorar la eficacia de la asistencia sanitaria a través de la eSalud; facilitar la participación de los ciudadanos mediante el acceso a información sanitaria de calidad, y ejecutar y compartir las mejores prácticas de telemedicina.

En 2008 se ratifica el compromiso de la UE con la telemedicina[169] y en la actualidad el ya citado plan i2010 incorpora diferentes elementos vinculados con esta materia atendiendo a lo marcado por el Plan de acción a favor de un Espacio Europeo de la Salud Electrónica[170]. Tras exponer las ventajas del empleo de la salud electrónica para todos los agentes implicados en la prestación del servicio sanitario, este plan marca una serie de objetivos a cumplir a largo plazo, consciente de que las transformaciones son procesos lentos. Señala como retos y líneas de actuación concretas la promoción del liderazgo de las autoridades políticas sanitarias, que deben comprometerse con la integración de la eSalud en sus países; la búsqueda de la interoperabilidad de los sistemas de información de los distintos países. Esta interoperabilidad ha de darse para hacer posible la identificación de los pacientes y el intercambio de información sanitaria en cualquier punto de la UE; el control de la movilidad de los pacientes; la mejora de la infraestructura y tecnologías, sobre todo la implantación generalizada de la banda ancha; la implantación de reglas que garanticen la calidad de los productos empleados; impulsar la inversión; y crear un marco jurídico adecuado que garantice la seguridad jurídica, sobre todo en materia de confidencialidad. Probablemente uno de los mayores retos que se planteen a nivel europeo es el de la interoperabilidad de los sistemas de información, con el fin de que la información pueda fluir entre los diferentes estados. En esta línea la recomendación de la Comisión sobre interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos marca una serie de pautas que los diferentes estados miembros deberían seguir: compromiso político y organizativo, interoperabilidad técnica y semántica, protección de los datos

[167] *The Contribution of ICT to Health,* Ministerial Conference and Exhibition, 22-23 mayo, en Bruselas, http://europa.eu.int/information_society/eeurope/ehealth/conference/2003/text_en.htm

[168] "*Ministers declared their wellingness to work together towards best practices in the use of ICT as tools for enhancing health promotion and health protection, as well as quality, accesibility and efficiency in all aspects of health care delivery*".

[169] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité del as Regiones de 4 de noviembre de 2008, "La telemedicina en beneficio de los pacientes, los sistemas sanitarios y la sociedad".

[170] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité del as Regiones, "La salud electrónica-hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica, 30 de abril de 2004.

sanitarios, sensibilización y educación[171]. La útlima referencia sobre esta cuestión en el ámbito europeo es la declaración de la conferencia Cooperación Europea sobre eHealth[172]. En esta declaración se refrendan los compromisos adoptados previamente, fundamentalmente sobre la necesidad de encontrar la interoperabilidad y crear un marco jurídico seguro para la transmisión de datos sanitarios[173].

En definitiva, la política europea, en lo que concierne a la telemedicina, se dirige básicamente a establecer unos criterios comunes en el ámbito de la UE que posibiliten el intercambio de información de una forma segura y rápida, con el objetivo de dar una asistencia sanitaria de calidad en cualquier lugar y momento[174].

En el Estado el "Plan España.es", dentro de la línea de actuación "administración.es", valoraba la sanidad como uno de los sectores de servicios públicos que mayor impacto puede tener en el desarrollo de la sociedad de la información. Por ello, el plan incidía en la necesidad de actuar de forma coordinada entre las distintas Comunidades Autónomas para la consecución de los principales objetivos en esta área, que no eran otros que la implantación de la Tarjeta Sanitaria Electrónica e intercambio de datos del Sistema Nacional de Salud; la Historia Clínica Unificada y su acceso a través del Sistema Nacional de Salud; Fondos de cohesión entre Comunidades Autónomas y compensación de actos médicos sobre no residentes; Redes de Emergencias Sanitarias; Servicios de Información en línea multiplataforma sobre Salud Pública y servicios sanitarios para los ciudadanos y servicios de Telemedicina y Teleasistencia sobre redes de banda ancha.

En esta dirección se dirigían los distintos proyectos que dentro de la iniciativa PISTA (Promoción e Identificación de Servicios emergentes de Telecomunicaciones Avanzadas)[175] se centraban en la sanidad: Intranet para un área asistencial, Intranet para un área de salud pública, trabajo colaborativo en entornos clínicos, sistema nacional integral de salud pública, receta electrónica y gestión farmaceútica, receta electrónica II, aplicación interactiva de productos farmaceúticos, y gestión del conocimiento científico. A día de hoy, en el marco del plan avanza, se está incidiendo sobre estos aspectos con el fin de desarrollar los diferentes servicios sanitarios a través de Internet, propiciando una mejor asistencia y, sobre todo, una mayor movilidad de los pacientes por todo el territorio estatal. Dentro del programa Sanidad en Línea el avance en la implantación de la receta electrónica y la historia electrónica resulta evidente, debiendo subrayarse que en la actualidad más de un 40% de farmacias pueden dispensar medicamentos electrónicamente a nivel estatal y que más de un 90% de los centros de salud del sistema

[171] Recomendación de la Comisión, 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos.
[172] Declaración "Cooperación Europea sobre eHealt", adoptada el 15 de maro de 2010 en Barcelona.
[173] VVAA, "El Reto de la Telemedicina en Europa", junio-julio 2010, en http://ec.europa,eu/
[174] WILSON, LEITNER, MOUSALLI, *Mapping the potential...*, cit., 2004: "*The European Council, in signing off this action, made clear that Europeans have the right to expect the following: to use information society tools to obtain reliable health information; that their health service providers have a strong backbone of eHealth infraestructure to allow the secure sharing of their Electronic Medical Record; and that there shohuld be European Union level coordinated responses to health threats*".
[175] http://www2.mityc.es/.

nacional de salud dispone de un sistema de historia clínica electrónica[176]. Los próximos proyectos se centran sobre todo en crear la posibilidad de intercambiar información clínica entre CCAA a través del Nodo Central del Sistema Nacional de Salud, de crear un sistema de intercambio de información asociada a las recetas electrónicas entre las CCAA a través del mismo Nodo, y promover los proyectos autonómicos de historias clínicas y recetas electrónicas[177]. El Plan de Calidad para el sistema de salud 2006-2010 incluye el programa sanidad en línea y en el mismo se marcan una serie de objetivos que tratan de consolidar la e-salud en el ámbito estatal: garantizar la identificación inequívoca de cada ciudadano en cualquier punto del Sistema Nacional de Salud; disponer de forma habitual de un sistema de intercambio y acceso a información clínica entre diferentes profesionales, dispositivos asistenciales y Comunidades Autónomas; impulsar la receta electrónica para su extensión en el Sistema Nacional de Salud; garantizar la accesibilidad desde cualquier punto del sistema, la interoperabilidad y la explotación adecuada de la información. Para cumplir con estos objetivos se plantean diferentes áreas de actuación vinculadas a compatibilizar los distintos sistemas de tarjeta sanitaria, historia elctrónica y receta electrónica en la esfera del sistema nacional de salud.

En lo que se refiere a la CAPV la eSalud también ocupa un espacio importante. Así, en el anterior Plan Euskadi en la Sociedad de la Información/Euskadi Informazio Gizartean 2002-2005, la eSalud se erigía en uno de los ámbitos de actuación más relevantes. Desde un punto de vista interno los objetivos eran la formación de los profesionales, crear un sistema que favoreciera la comunicación entre profesionales, mejorar el sistema de información para que garantizara la homogeneidad, seguridad y confidencialidad de los datos tratados y centralizara y agilizara los contratos, pedidos, facturas etc. con los proveedores y clientes. A nivel externo, el objetivo era facilitar la relación asistencial: facilitar la identificación del paciente y la comunicación, y crear nuevas formas de informar, educar y entretener al paciente. Para ello, los principales proyectos en lo que respecta a la salud en la CAPV se centraban en la implantación de la Tarjeta Sanitaria/Ciudadana electrónica, Historia Digital Única, Receta Electrónica y Portal de Sanidad. En el último Plan Euskadi en la Sociedad de la Información “La Agenda Digital de Euskadi 2010” no hay una referencia expresa a esta cuestión, pero en numerosas ocasiones se cita dentro del proyecto de crear una Administración electrónica eficiente, la importancia de integrar las nuevas tecnologías en el sector sanitario.

La apuesta en la CAPV por la implantación de las TIC en el ámbito sanitario público es clara. Así quedaba fijado ya en el Plan Estratégico de Osakidetza 1998-2002[178] en el que, como señaló el entonces Consejero de Sanidad[179], el desarrollo tecnológico se consideraba como uno de los cinco grandes objetivos estratégicos. Así quedaba recogido también en el Plan Estratégico 2003-2007 de Osakidetza en el que, al igual que en el anterior, las nuevas tecnologías ocupaban un papel fundamental para la mejora de la calidad del servicio sanitario en todas sus vertientes. En la actualidad, tanto el Plan de Modernización y Adecuación de Infraestructuras y Equipamientos

[176] Informe ONTSI (Observatorio Nacional de las Telecomunicaciones y la SI) “La Sociedad en Red”, 2009, http://www.ontsi.red.es.
[177] Red.es, “Las TIC en el Sistema Nacional de Salud”, enero de 2010.
[178] http://www.osanet.euskadi.net/
[179] Comparecencia del Consejero de Sanidad, Iñaki AZKUNA en la Comisión de Trabajo y Sanidad, el 04/05/1998 para infomar sobre el Plan Estratégico 1998-2002 de Osakidetza. En http://parlamento.euskadi.net/.

del Sistema Sanitario Público Vasco para 2007-2012, como el Plan Estratégico de Osakidetza para 2008-2012, marcan las pautas a seguir en el desarrollo de las líneas de actuación ya señaladas en planes o proyectos anteriores: fundamentalmente, hacerse con los equipos tecnológicos más avanzados, con el fin de alcanzar una mayor eficiencia en el uso de las TIC y desburocratizar los procesos asistenciales con herramientas como la receta electrónica; continuar en el proceso ya iniciado de desarrollo de la historia clínica única e informatizada, con el fin de integrar y coordinar la atención primaria y especializada[180].

La informatización de Osakidetza tiene comienzo en la década de los 80, si bien los Sistemas de Información residían, por aquel entonces, en arquitecturas diferentes, lo que llevaba a que se formaran islas de información. En los 90 los Sistemas de Información de Osakidetza comienzan a evolucionar hacia Sistemas Integrados de Información impulsados por el denominado Plan Estratégico del Sistema de Información Sanitaria (PESIS) que marcará el camino a seguir para los siguientes avances[181], que se llevarán a cabo, primero en el marco del llamado programa OMI-AP, y después, a partir de finales de 1998, con el vigente Plan Osabide, que pretende informatizar los Sistemas de Información de la Atención Primaria (3s-Osabide) y los de la Atención Especializada (e-Osabide) con el fin último de conseguir una base de datos única y común, un Sistema Integrado de Información para todo el sistema sanitario. Junto a esta transformación integral, los cambios en el sistema sanitario vasco se producen en relación a proyectos concretos como los de la receta electrónica, ya implantado en diferentes centros y farmacias, la historia clínica electrónica, también en proceso de implantación, y la tarjeta sanitaria electrónica, que debido al proyecto ONA ha contado con un impulso importante.

III.2.3. Aspectos positivos y negativos de la implantación de las TIC en la sanidad.

III.2.3.A.Ventajas.

Las ventajas que las TIC aportan a los distintos ámbitos de actuación del servicio sanitario son múltiples, derivadas de todas las aplicaciones que estas nuevas tecnologías tienen en este sector: Historia de Salud Electrónica, Tarjetas Sanitarias Inteligentes, Recetas Electrónicas, etc[182]. Cabe apuntar desde ahora que todos estos proyectos responden a un objetivo común, que persigue la telemedicina como nueva forma de ejercer la sanidad y que constituye a su vez su principal ventaja. Se trata de potenciar un servicio sanitario de calidad. Las posibilidades que

[180] http://www.osakidetza.euskadi.net/
[181] Memoria Osakidetza 1999.
[182] WILSON, LEITNER, MOUSALLI, *Mapping the potential...*, cit., 2004, pp. 27-30, realizan un interesante y completo estudio sobre las ventajas que aportan las TIC a los ciudadanos, a éstos cuando se convierten en pacientes, a los profesionales, y al centro en general para realizar tareas de gestión.

ofrecen las TIC deberían acarrear como consecuencia directa una mejor asistencia sanitaria[183], lo que redundaría de forma positiva en el derecho que la CE reconoce a la protección de la salud[184].

Centrándose en aspectos más concretos, una de las aplicaciones más ventajosas de las TIC es la creación de un sistema de comunicación basado en Intranets e Internet que posibilita una relación continuada, directa y ágil entre profesionales, y entre éstos y pacientes. La posibilidad de que esta comunicación se lleve a cabo plantea una serie de ventajas, desde un punto de vista puramente práctico, que merecen ser destacadas[185].

Primero, la especialización de los profesionales sanitarios ha llevado a que sus conocimientos cada vez se limiten más a un aspecto concreto de la práctica médica, lo cual hace que sea imprescindible la comunicación rápida entre ellos para la resolución de dudas o para pedir segundas opiniones[186]. Esta necesidad se ve satisfecha gracias a las TIC, pudiendo incluso transmitir imágenes en tiempo real, facilitando que la colaboración entre profesionales resulte más efectiva[187]. Una mayor comunicación supondrá que se comparta conocimiento y que consecuentemente éste aumente, lo cual traerá una mejor asistencia.

Segundo, las posibilidades de comunicación y cooperación hacen que sea factible que todos los niveles asistenciales y todas las áreas de atención se integren, incluso la farmaceútica[188], llegando así a lo que se ha venido en llamar la *sharing care*[189]. Esta integración hace que todo un proceso asistencial se lleve a cabo como un único acto médico, sin que cada operación se vea de manera aíslada y desvinculada con los demás.

Tercero, y más allá de los beneficios que pueda plantear la e-salud desde el punto de vista interno, para el funcionamiento de un sistema sanitario las posibilidades de fomentar y potenciar la comunicación tienen su aplicación positiva en la relación médico-paciente. Más que la comunicación entre profesionales se ha apuntado como una de las principales ventajas de las TIC la comunicación entre profesionales y pacientes vía, sobre todo, correo electrónico[190] y, ahora, teléfonos móviles de tercera y cuarta generación. La posibilidad de practicar una comunicación inmediata a distancia entre estos dos sujetos hace, en primer lugar, que el paciente sólo tenga que acudir al médico cuando sea absolutamente necesario, pudiendo este último aclarar dudas que el paciente pueda tener a distancia (tele-consulta), lo que es

[183] SÁNCHEZ FIERRO, "Los nuevos...", cit., p.8, llega a cuantificar las vidas que se salvarían empleando las TIC atendiendo a informes realizados en los EE.UU. "Un informe del *Institute of Medicine* de USA señala que casi 100.000 personas salvarían la vida al año si los profesionales de ese país contasen con una adecuada gestión de la información y del reconocimiento sobre tratamiento, dosificación, prevención, contramedicaciones etc.". "Otro estudio del Servicio de Salud Británico afirma que 16.000 vidas podrían prolongarse contando los profesionales con información permanente sobre el cáncer".
[184] Artículo 43 CE.
[185] MORENO VERNIS, "Documentación Clínica…", cit., 2002, pp. 56-57.
[186] CRESPO del ARCO, "Aplicaciones Médicas…", cit., 1998.
[187] SÁNCHEZ CARO, "El uso y acceso a la historia…", cit., 2010, p. 1.070.
[188] MAYORAL BENITO, "Salud e Internet...", cit., 2001, p. 26. "Las nuevas tecnologías permitirán al titular de la oficina colaborar con otros profesionales y con las autoridades sanitarias mediante su interconexión telemática".
[189] MARIMÓN, *La Sanidad...*, cit., 1999, p. 195: "cooperación entre profesionales (médicos, enfermeras, farmaceúticos, asistentes sociales,...) de diversas unidades proveedoras de servicios de salud".
[190] MAYER PUJADAS y LEIS MACHÍN, "El Correo Electrónicio…", cit., 2006.

especialmente valioso en casos de enfermedades crónicas[191], ganándose tiempo tanto para el paciente como para el médico. Una comunicación más continuada y rápida entre médico y paciente supondrá, en segundo lugar, una mayor participación del paciente en la terapia haciendo que éste se sienta integrado en el proceso asistencial y posibilitando que el médico tenga un mayor conocimiento del problema concreto del paciente[192], lo cual, evidentemente, favorece el servicio. Esta relación médica en el ciberespacio supone el complemento perfecto, ágil y continuo a la principal relación física entre profesional y paciente[193].

La posibilidad de atender a los pacientes a distancia superando toda barrera espacial y/o estructural trae consigo otra serie de ventajas. En primer lugar, se convierte en una alternativa a la masificación que debido a la tendencia que en los últimos años ha ido adquiriendo la curva demográfica sufren los centros[194], permitiendo gestionar de manera más eficaz las camas hospitalarias[195]. En segundo lugar, las TIC permiten que la asistencia llegue a lugares de difícil acceso o alejados de las grandes ciudades, convirtiéndose en una vía para garantizar la igualdad real entre la ciudadanía[196]. Por último, la asistencia en el domicilio que posibilitan las nuevas tecnologías conlleva la humanización del proceso asistencial, en la medida en que el servicio se presta en el domicilio, lo cual permite mayor intimidad y comodidad, la integración de la familia en el proceso, evita posibles infecciones y depresiones en el hospital, etc[197]. En términos generales, puede deducirse que las distintas aplicaciones que la telemedicina tiene en la asistencia a distancia permiten una mayor integración del paciente y su familia en el proceso asistencial, lo que favorece algo tan importante como la autonomía del paciente[198].

Otro de los aspectos que hay que resaltar como positivos en la implantación de las TIC en el ámbito sanitario se refiere a la integración de la información sobre el paciente[199]. En más de una ocasión se ha afirmado que la clave del progreso en la sociedad de la información en el ámbito de la sanidad reside en la integración[200]. Las nuevas tecnologías permiten que la información del paciente proveniente de diferentes fuentes, independientemente del formato (foto, video, texto, voz...), se incorpore a una sola base de datos, que será la Historia de Salud Electrónica.

---

[191] Entrevista a J. REIG REDONDO, "El futuro...*",* cit., 2000.
[192] MAYORAL BENITO, "Salud e Internet...", cit., 2001, pp .25-26.
[193] JACQUEMIN, "La Telemedicina...", cit., 2003.
[194] GONZÁLEZ RAMALLO, VALDIVIESO MARTÍNEZ y RUIZ GARCÍA, "Hospitalización a domicilio...", cit., 2002, p. 659.
[195] ESCARRABILL, "La Atención...", cit., 2002, p. 96: "En la mayoría de éstos hospitales se está produciendo una reconversión de las camas convencionales para dedicarlas a otros usos distintos de la hospitalización convencional: unidades de corta estancia, hospital de día, cuidados intermedios. Esto ha permitido incrementar la eficiencia de los hospitales".
[196] SOLER-GONZÁLEZ, RIBA TORRECILLAS, RODRÍGUEZ-ROSICH, SANTAFÉ SOLER y BUTI SOLE, "Aplicaciones de Tecnología...", cit., 2004, p. 175.
[197] GONZÁLEZ RAMALLO, VALDIVIESO MARTÍNEZ y RUIZ GARCÍA, "Hospitalización a domicilio...", cit., 2002, p. 661.
[198] FERRER ROCA, *La Telemedicina...*, cit., 2001, pp. 47-48, explica las distintas aplicaciones que las TIC pueden tener en este sentido.
[199] MÉJICA GARCÍA, *El Enfermo Transparente…*, cit., 2002, p. 15.
[200] MARIMÓN, "*El progreso...*", cit., 2002, p. 134: "Existe una relación de dependencia entre el nivel de integración de la información y reducciones de tiempo, de reiteraciones (de introducción, acceso o generación de informaciones) y de errores (en datos e interpretaciones); por tanto, la posibilidad de mejoras organizativas y de productividad depende de la integración. Igualmente, la capacidad de interpretación de la información, base del conocimiento, se multiplica en función del nivel de integración de la sinfomraicones generadas y accesibles".

Las ventajas que plantea esta posibilidad son evidentes: se evitan las islas de información relativas a un paciente que haya podido pasar por distintos centros o áreas de asistencia; se evitan duplicidades, lo que facilita el control de los responsables de los ficheros; se facilita la actualización de la información; se facilita la estructuración de la información de forma que su interpretación sea rápida y sencilla; se facilita el proceso de transformación eficiente de los datos en información[201]; se posibilita que el paciente pueda tener acceso a toda la información relativa a su salud y que pueda corregir posibles errores, etc. La viabilidad de contar con una información completa, clara, estructurada, actualizada y fácil de interpretar, es una ventaja subrayable que aportan las TIC a los profesionales de la sanidad.

La aplicación de la telemática a las bases de datos sanitarias facilita también el acceso a los mismos por parte de los profesionales sanitarios. Las TIC hacen posible que los profesionales sanitarios tengan un acceso rápido y ágil a la información del paciente desde cualquier lugar y en cualquier momento y que esta información esté estructurada de tal forma que responda a necesidades concretas, por ejemplo a casos de urgencia donde la inmediatez supone un valor añadido[202], o para la realización de estadísticas, o investigaciones, o controlar los gastos. Además, se posibilita el acceso por distintos profesionales a los mismos recursos[203]. Las nuevas tecnologías, por otro lado, hacen posible que este acceso sea controlado. Primero, porque permite que se controlen todos los accesos que se hayan podido producir sobre la documentación sanitaria. Y segundo, porque hace viable que cada uno de los usuarios del sistema de información sanitaria sólo pueda tener acceso a los datos necesarios para el cumplimiento de sus funciones. Estas posibilidades repercuten en una mejor salvaguarda de la confidencialidad de los datos sanitarios.

Por último, resulta destacable la posibilidad que ofrecen las TIC de acceder a una mayor cantidad de información especializada sobre la salud, tanto para los profesionales como para los ciudadanos en general. En el caso de los profesionales la necesidad de acceder a fuentes de información resulta evidente. Para realizar investigaciones concretas o en la práctica médica diaria, para conocer las causas de los problemas de salud, el tratamiento correcto etc., es imprescindible que el médico tenga a su disposición información a este respecto de forma rápida y útil[204], cosa que se hace posible con las TIC a través de bibliotecas virtuales o el acceso a Internet en general. En lo que respecta a los pacientes, hay que apuntar que cada vez son más las páginas *web* relativas a la salud que ofrecen información concerniente a esta materia y que cada vez son más las personas que visitan estas páginas[205]. Así, los ciudadanos están cada vez más informados, tienen la posibilidad de contrastar lo que les dicen los profesionales y participan

[201] ALONSO LÓPEZ y GANCEDO GONZÁLEZ, "Informatización Integral...", cit., 1999, p.282.
[202] LÓPEZ GONZÁLEZ, "Documentación Clínica...", cit., 1998.
[203] GARCÍA-BARRERO, "Telemedicina en Europa...", cit., 2000, pp. 43-45.
[204] ARZA y GRANDES ODRIOZOLA, "*Podemos superar...*", cit., 1998.
[205] WILSON, LEITNER, MOUSALLI, *Mapping the potential...*, cit., 2004, p. 17. Al rededor del 40% de los europeos usan Internet para buscar información sobre la salud.

más activamente en el proceso asistencial. Dicho esto, no se puede dejar de subrayar el riesgo de que la información a la que se accede por estos medios sea de dudosa calidad[206].

Se podría decir que las citadas constituyen las ventajas más reseñables que las TIC aportan al ámbito sanitario. Sin embargo, cada proyecto concreto, Historia de Salud Electrónica, Tarjeta Sanitaria Inteligente, Receta Electrónica, trae consigo, a su vez, otros aspectos positivos que luego se destacarán.

III.2.3.B. Desventajas.

La aplicación de las TIC en el campo sanitario plantea una serie de problemas que, en la medida en que no son insalvables, no se pueden considerar, al menos la mayoría de ellas, como verdaderas desventajas, pero que hay que tener en cuenta al trazar un plan para la implementación de las nuevas tecnologías en los centros sanitarios.[207]

La primera de las cuestiones a tener presente es la de la legitimación de estos nuevos instrumentos[208], es decir, la necesidad de demostrar que las TIC constituyen herramientas más eficientes que otras para llevar a cabo la actividad sanitaria. En este sentido, son los profesionales de la sanidad los que en primer lugar tienen que convencerse de la validez y mayor eficacia de las TIC, ya que en última instancia serán ellos los que junto a la Administración tendrán que impulsar a los ciudadanos a emplear las nuevas tecnologías en su relación con la Administración, en general, y con los centros sanitarios en particular. "*The reasonable man adapts himself to the world, the unreasonable one persists in trying to adapt the world to himself. Therefore, all progress depends on the unreasonable man*"[209]. Estas palabras de GB. SHAW exponen magistralmente la dependencia del proceso de mecanización con respecto de la actitud de los profesionales sanitarios.

En algún caso la doctrina ha señalado el carácter conservador y cauto de los profesionales sanitarios con respecto a las TIC[210]. Sin embargo, tampoco faltan estudios que apuntan en sentido contrario, exponiendo el interés de este colectivo por introducir nuevas tecnologías de información y diagnóstico, entendiendo como prioritarias la incorporación de las redes de internet e intranet, redes que faciliten el acceso a la información de laboratorios y radiología, así como otras que faciliten el acceso a atención primaria y a especialidades, destacando también la necesidad de informatizar la Historia Clínica[211].

La eSalud supone una nueva forma de trabajar para los profesionales, no sólo por los nuevos instrumentos que van a emplear, sino por la relación que va a formarse entre médico y paciente,

[206] Entrevista a REIG REDONDO, "El Futuro...", 2000; AMENGUAL PLIEGO, "Información científica…", cit., 2004; MIRA, PÉREZ-JOVER y LORENZO, "Navegando en Internet…", cit., 2004.
[207] MÉJICA GARCÍA, *El Enfermo Transparente…*, cit., 2002, p. 21.
[208] HERRANZ RODRÍGUEZ, "Aspectos éticos...", cit., http://2000, www.aeds.org/.
[209] WILSON, LEITNER, MOUSALLI, *Mapping the potential...*, cit., 2004, p. 28, recogen esta expresión. En castellano: "El hombre razonable adapta su forma de ser al mundo, el irrazonable persiste en adaptar el mundo a su forma de ser".
[210] DEL POZO GUERRERO y GÓMEZ AGUILERA, "Telenedicina: una visión…", cit., 2001, p. 458.
[211] BLEDA, DE SEBASTIÁN y ROVIROSA, "Estudios sobre la actitud...", 1999.

más directa y continuada. Las TIC exigen al profesional tener que adaptarse a estas herramientas y, sobre todo, a un mayor protagonismo del paciente[212]. La inevitable adaptación a las TIC supone una barrera que sólo se superará mediante la formación de los profesionales en el uso de las mismas. Se ha llegado a afirmar que el verdadero problema a la hora de implantar las nuevas tecnologías en el ámbito sanitario, no es tanto el económico "sino de planteamiento y de formación por parte de las partes implicadas"[213], por lo que establecer mecanismos de formación tanto para profesionales en activo, organizando cursos, como para estudiantes, adaptando el plan de estudios a las nuevas circunstancias, se antoja como algo fundamental[214]. La formación, la actualización del conocimiento, tiene que ser un compromiso individual de cada profesional, que tiene que aplicarse en el proceso de adaptación, pero también de las organizaciones y autoridades que intervienen en la regulación de la profesión, que tienen que poner todos los medios para que la adaptación sea posible[215].

Más allá de su relación con las nuevas tecnologías, el profesional tendrá que cambiar también la mentalidad en su relación con el paciente. El "enfermo informado" constituye hoy día una realidad en la práctica sanitaria[216]. Se trata de un ciudadano con mayores conocimientos sobre su salud, que exige una mayor participación en el proceso curativo (y que cuenta con los medios para ello) y una mejor asistencia[217]. A estas características habría que añadir que el enfermo es también cada vez más consciente de su intimidad y del derecho a la autodeterminación informativa ante actuaciones que tiempos atrás podrían ser comunes en el sector sanitario, como las conversaciones entre profesionales sanitarios en las que se vulnera la confidencialidad o la exposición de datos sanitarios en tablones de los centros, pero que hoy día empiezan a verse con cierta cautela[218]. Los profesionales tienen que lograr que la relación médico-paciente no se vea deteriorada, aunque cambie, por el uso de las TIC. La telemática tiene que servir para acercar a médicos y pacientes y no para alejarlos[219].

En segundo lugar, desde un punto de vista eminentemente técnico, los obstáculos a superar son varios. La barrera más significativa en este sentido es la de la seguridad de la información relativa a la salud. Este punto se ha puesto de manifiesto recientemente en un informe de la AEPD, que subraya los problemas de los centros sanitarios para cumplir con el principio de seguridad dispuesto en la LOPD[220]. Las posibilidades que aportan las TIC no pueden ejecutarse

[212] MAYORAL BENITO, "Salud e Internet...", cit., 2001, p. 26.
[213] TOMÁS, "La Implantación...", cit., 2003.
[214] GARCÍA ROJO, "Formación Médica...", cit., 2001, pone de manifiesto, en primer lugar, la necesidad de formar a los profesionales en TIC, y en segundo lugar, las posibilidades que las propias TIC ofrecen para llevar a cabo dicha formación. Y es que hay que subrayar que en una materia como la sanitaria, en la que el conocimiento actualizado es algo imprescindible, las TIC pueden constituir un aliado muy valioso.
[215] En este sentido cabe destacar el compromiso que exige el Código de Ética y Deontología Médica de 1999, en su art. 21.1: "*El ejercicio de la medicina es un servicio basado en el conocimiento científico, en la destreza técnica y en las actitudes éticas, cuyo mantenimiento y actualización son un deber individual del médico y un compromiso de todas las organizaciones y autoridades que intervienen en la regulación de la profesión*".
[216] "Conclusiones sobre las II Jornadas Nacionales sobre Internet y Salud Infors@alud-net.2000", *Informática y Salud* nº 26, mayo-junio 2000, http://www.seis.es/.
[217] TOLOSA ASENJO, "Gestión hospitalaria…", cit., 2006, pp. 121-122.
[218] SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000, p. 192.
[219] HERRANZ RODRÍGUEZ, "Aspectos Éticos...", cit., 2000.
[220] Informe jurídico de la AEPD, "Informe de cumplimiento de la LOPD en Hospitales", octubre de 2010.

sin un sistema de información seguro, capaz de generar confianza. Esta idea se refuerza aquí por el hecho de que se está en un ámbito en el que se manipula información la mayoría de las veces muy sensible, con lo que un mal uso de dichos datos puede acarrear consecuencias especialmente gravosas para sus titulares[221]. La garantía de la confidencialidad de los datos sanitarios ha de ser una constante en la práctica sanitaria[222]. Esta necesidad se ha subrayado en numerosas ocasiones[223], no sólo como fundamento de la protección del derecho a la autodeterminación informativa, sino también como instrumento indispensable en la consolidación de una fortalecida relación de confianza entre paciente y profesional sanitario[224].

La seguridad 100% en un sistema de información es inexistente[225], sin embargo, todavía hoy, la desconfianza en las TIC para realizar distintas operaciones parece seguir siendo mayor que en los sistemas basados en papel, situación en todo caso injustificada pues la manipulación de información en formato papel plantea desde todos los puntos de vista mayores problemas[226]. Hay que tratar de minimizar los riesgos, y en este sentido las TIC aportan soluciones concretas y reales.

En lo que aquí interesa, una de las desventajas principales se traduce en que la aplicación de la telemática a la sanidad y el empleo de las nuevas tecnologías para manipular información relativa a la salud generan nuevos riesgos para la integridad y seguridad de los datos[227]. Las TIC

[221] I Jornada de Sistemas de Información en Salud Laboral, "La seguridad como tecnología básica para la salud laboral", *Informática y Salud*, nº35, marzo 2002. "En general y según todas las encuestas e informaes realizados, existen básicamente dos impedimentos que frenan el uso masivo de la realización de trámites a través de Internet: la seguridad y confianza (considerado el principal obstáculo por el 70%)", http://www.seis.es/. DE MIGUEL SÁNCHEZ, *Secreto médico…,* cit., 2002, p. 260.

[222] GRACIA GUILLÉN, *La Confidencialidad…,* cit., 2000, p. 19; LÓPEZ CARMONA, "e-Salud, Confidencialidad…", cit., 2006, pp. 95-96, subraya que en la actualidad el respeto a la confidencialidad se encuentra sometido a nuevos retos.

[223] Declaración de Lisboa de la Asociación Médica Mundial sobre los Derechos del Paciente, 34ª Asamblea Médica Mundial, en Lisboa, septiembre/octubre 1981, enmendada en septiembre de 1995 y revisada en octubre de 2005, recoge como uno de sus principios el "Derecho al secreto: Toda la información identificable del estado de salud, condición médica, diagnóstico y tratamiento de un paciente y toda otra información de tipo personal, debe mantenerse en secreto, incluso después de su muerte. Excepcionalmente, los descendientes pueden tener derecho al acceso de la información que los prevenga de los riesgos de salud.
La información confidencial sólo se puede dar a conocer si el paciente da su consentimiento explícito o si la ley prevé expresamente eso. Se puede entregar información a otro personal de salud que presta atención, sólo en base estrictamente de "necesidad de conocer", a menos que el paciente dé un consentimiento explícito.
Toda información identificable del paciente debe ser protegida. La protección de la información debe ser apropiada a la manera del almacenamiento. Las substancias humanas que puedan proporcionar información identificable también deben protegerse del mismo modo".

[224] Declaración de la Asociación Médica Mundial sobre las consideraciones éticas de las bases de datos de salud, Washington, 2002: se refiere a la importacia de proteger los datos de salud con el fin de fortalecer la relación entre médicos y pacientes.

[225] LÓPEZ GONZÁLEZ, "Documentación Clínica...", cit., 1998, "deberemos valorar mucho el coste-beneficio" "a la hora de implantar un sistema de disposición de los documentos clínicos a través de Internet"

[226] Ténganse en cuenta como ejemplo, las múltiples apariciones de Historias Clínicas en la basura: Boletín de Noticias LOPDate, 22/01/04, 17/01/03, 22/01/03, 05/02/03, etc. en http://www.lopdate.com/.

[227] PÉREZ-CAMPANERO ATANASIO, "La Gestión...", cit., 2000, pp. 97-133, en un brillante trabajo fija los riesgos comunes para la seguridad de los sistemas de información y de las comunicaciones: acceso no autorizado, caballo de Troya, monitorización de las comunicaciones, simulación, denegación de acceso, repudio, rastreo, prueba y error, obtención de contraseñas, abortar programas, gusanos y bombas lógicas, a los que habría que añadir, como apuntan SANZ URETA y HUALDE TAPIA, "Aspectos Técnicos...", cit., 2000, p. 75-76, problemas físicos (sobrecargas eléctricas e interrupciones de alimentación, temperaturas extremas, etc.) y catástrofes (inundaciones, incendios...).

hacen posible un mayor flujo de información a escala incluso internacional. La aplicación de la telemedicina implica que haya más información y que su uso y, sobre todo, movimiento se dé a mayor escala. Las propias leyes reconocen supuestos en que este flujo de datos sanitarios se haya de producir para que las aplicaciones de la telemedicina sean posibles[228]. Esto conlleva el riesgo de que, a su vez, haya más posibilidades de accesos, transmisiones y alteraciones incontroladas[229]. Obviamente, cuanto más se empleen los datos y más se transfieran entre diferentes órganos, mayor será el peligro de que se produzca un mal uso de los mismos. Son conocidos los supuestos en que datos sanitarios de pacientes han acabado publicados en Internet debido a descuidos o a la mala fe de empleados que han tratado de utilizar los datos de manera contraria a Derecho[230]. No obstante la veracidad de esta afirmación, hay que enfrentar a este problema el argumento de que si bien hay nuevos peligros, también hay más soluciones para garantizar la autentificación (identificación del usuario), autorización (determinar lo que el identificado puede hacer), disponibilidad (que los sistemas funcionen el mayor tiempo posible), confidencialidad, integridad y no repudio (que quede constancia de las transacciones)[231].

Se trata de riesgos que pueden crear, como afirma PÉREZ-CAMPANERO ATANASIO, "La Gestión...", cit., 2000, 4 tipos de problemas: violación de la privacidad de la información, destrucción o modificación de la información, uso de servicios sin sutorización, o control del sistema; SÁNCHEZ CARO y SÁNCHEZ CARO, *El Médico…,* cit., 2001, p. 134; DORADO y FERNÁNDEZ-HERRERA, "La protección de datos…", cit., 2006.

[228] Artículo 53 Ley 16/2003, 28 de mayo de cohesión y calidad del Sistema Nacional de Salud: "*1. El Ministerio de Sanidad y Consumo establecerá un sistema de información sanitaria del Sistema Nacional de Salud que garantice la disponibilidad de la información y la comunicación recíprocas entre las Administraciones sanitarias (...);5. Las comunidades autónomas, la Administración General del Estado y las Entidades Gestoras de la Seguridad Social aportarán a este sistema de información sanitaria los datos necesarios para su mantenimiento y desarrollo. Del mismo modo, las Administraciones autonómicas y estatal tienen derecho de acceder y disponer de los datos que formen parte del sistema de información que precisen para el ejercicio de sus competencias*".

Artículo 56 Ley 16/2003, 28 de mayo de cohesión y calidad del Sistema Nacional de Salud: "*Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione.*

El Ministerio de Sanidad y Consumo establecerá un procedimiento que permita el intercambio telemático de la información que legalmente resulte exigible para el ejercicio de sus competencias por parte de las Administraciones públicas.

El intercambio de información al que se refieren los párrafos anteriores se realizará de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en la Ley 41/2002, de 14 de noviembre".

[229] MARIMÓN, *La Sanidad...,* cit., 1999, p. 298; SOLERNOU VIÑOLAS, "Aspectos legales y éticos…", cit., 2006, p. 47.

[230] SAN 11 de febrero de 2010, en la que se enjuicia el supuesto en que datos de numerosos pacientes aparecen publicados en Internet.

[231] Que es lo que se quiere conseguir con el empleo de TIC de Seguridad (TIC_S), como afirman SANZ URETA y HUALDE TAPIA, "Aspectos Técnicos...", cit., 2000, p. 76 plantean una política de seguridad basada en cuatro líneas de actuación: mecanismos de prevención que garantizan la seguridad del sistema durante su uso habitual; mecanismos de detección; mecanismos de recuperación; y mecanismos de auditoría.

PÉREZ-CAMPANERO ATANASIO, "La Gestión...", cit., 2000, pp. 104-110: Se trata de medidas que tratan de garantizar la seguridad externa (la que hace referencia a los mecanismos dirigidos asegurar la inviolabilidad del sistema informático en cuanto a las posibles intrusiones que pudieran producirse sin intervención del sistema, o fallos o errores que, debiéndose al sistema, no pueden ser controlados por el mismo) , interna (dirigida a que los usuarios del sistema, o los extraños que hayan podido tener acceso al mismo, no puedan manipular la información contenida en el mismo para la cual no están autorizados) y funcional (problemas de seguridad que suscitan las líneas de comunicación y el funcionamiento anormal del propio sistema debido a fallos y caídas) del sistema.

La seguridad en los sistemas de información, entendida como "la característica de un sistema que lo hace ser capaz de proteger sus datos frente a la destrucción, interceptación o modificación no deseadas"[232], sólo es posible implantando un plan integral que abarque todos los aspectos: jurídico, técnico y de formación, que exija la actuación de todos los actores implicados. A esta cuestión se le ha dado especial relevancia desde todos los foros, especialmente desde el científico, pero también desde el jurídico[233]. La implantación de un sistema de seguridad eficiente tiene como principal obstáculo el elevado coste de las infraestructuras necesarias para garantizar un nivel aceptable de la misma. Además, hay que tener en cuenta que las TIC están en constante evolución y que probablemente la necesidad de renovación será continua, pues la telemedicina depende por completo de las TIC. Un nuevo modelo de servicio sanitario, basado en TIC seguras, requiere de un compromiso político claro que tiene que reflejarse en inversiones en tecnología y personal cualificado.

Más allá del concreto aspecto de la seguridad, el hecho de que la telemedicina se erija como un proyecto más dentro de la sociedad de la información, que como antes se decía pretende tener un alcance universal, plantea desde un punto de vista técnico otros problemas reseñables. El carácter global que se le supone a esta nueva sociedad hace que la telemedicina se configure como una aplicación de carácter internacional, que es, por otro lado, la mejor forma de sacar partido a las posibilidades que ofrece el empleo de las TIC en el ámbito sanitario[234]. Sin embargo, si se quiere que la eSalud tenga el citado alcance para que la asistencia sanitaria sea igual de eficaz en cualquier lugar y en cualquier momento, será necesario implantar un sistema de información global en el que la información pueda fluir sin problemas, y para ello, serán necesarias tecnologías compatibles[235] y un lenguaje reconocible[236] para los distintos subsistemas, además de un marco normativo que dé respuesta a los problemas que puedan derivar precisamente de ese carácter internacional, sobre todo, en materia de responsabilidad[237].

En el ámbito estatal la compatibilidad entre los diferentes sistemas de información que se emplean en las comunidades autónomas y la Administración central viene exigida por el ordenamiento[238]. La solución a la falta de compatibilidad se puede lograr de diferentes formas. La interoperabilidad en el ámbito estatal se formaliza, por ejemplo, mediante convenios entre las

[232] SANZ URETA y HUALDE, "Aspectos Técnicos...", cit., 2000, p. 74.

[233] La propia LOPD, recoge en su artículo 9 la seguridad como un pilar fundamental en la protección de los datos personales.

[234] JACQUEMIN, "La Telemedicina...", cit., 2003, "si queremos aprovecharnos de todos los beneficios de la telemedicina, hay que considerarlo como una forma de practicar la medicina a nivel internacional".

[235] GARCÍA-BARBERO, "Telemedicina en...", cit., 2000, pp. 43-45: "el problema técnico más importante es la incompatibilidad de las redes que se están montando y la falta de definición de stándares técnicos". Señala el autor que "la lucha de la industria por hacerse con el mercado condiciona gran cantidad de programas piloto en distintas áreas, sin una visión de futuro en cuanto a la integración/coordinación de las distintas aplicaciones"

[236] CANO CERVIÑO, FERRER RIPOLLES, SIGNES ANDREU y TOLOSA FUERTES, "El Lenguaje...", cit., 2003.

[237] MÉJICA GARCÍA, *El Enfermo Transparente…*, cit., 2002, p. 65.

[238] DA Tercera LBAP: "*El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competetes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición*". En el mismo sentido Artículo 56 Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

distintas administraciones en los que se ponen de acuerdo para que el flujo de la información sea posible y las distintas herramientas de telemedicina se hagan efectivas, la historia clínica electrónica, tarjeta sanitaria y receta electrónica[239].

Atendiendo a los problemas que plantea la incorporación de las TIC en el ámbito sanitario en su conjunto, se está de acuerdo aquí con quienes tratan de incidir más en el aspecto humano que en el técnico[240]. Para que los avances tecnológicos puedan verse reflejados en la realidad será necesario formar a los profesionales y establecer protocolos de actuación que determinen un modelo de comportamiento para los mismos, de forma que el uso que hagan éstos de las TIC sea el adecuado, empleando las nuevas tecnologías cuándo y cómo sea oportuno[241], como por otro lado exige el Código de Ética y Deontología Médica de 1999 en una expresión muy poco afortunada y que hay que entenderla de forma no demasiado rigurosa: *"No son éticas (...); y el ejercicio de la Medicina mediante consultas exclusivamente por carta, teléfono, radio, prensa o Internet"*[242].

III.3. Herramientas concretas de Telemedicina.

Si bien en la telemedicina o eSalud se recogen numerosos instrumentos con distintas aplicaciones, se hará mención, solamente, a los proyectos que mayor relevancia han adquirido en los últimos años: Historia de Salud Electrónica, Tarjeta Sanitaria Inteligente, y Receta Electrónica.

III.3.1. La Historia de Salud Electrónica.

Siguiendo el contenido de la LBAP la historia clínica es, entre otras cosas, un conjunto de documentos e información sobre los procesos asistenciales de los pacientes[243]. Se erige por lo tanto en una base de datos de especial relevancia sobre el estado de salud física y mental de las personas. Es sabido que la historia clínica es uno de los instrumentos más importantes, si no el que más, para la prestación del servicio sanitario[244]. Primero, constituye un documento indispensable a la hora de otorgar asistencia sanitaria. Segundo, se trata de una base de datos cuyo empleo resulta necesario para la consecución de fines de investigación, de realización de estadísticas, de docencia, de gestión económica y administrativa, etc. La necesidad de que los distintos profesionales sanitarios puedan disponer de esta herramienta de una forma sencilla y rápida para llevar a cabo sus funciones adecuadamente es incuestionable.

[239] Resolución de 28 de octubre de 2009, de la Secretaría General de Sanidad, por la que se publica el Convenio de colaboración ente la Comunidad Autónoma del País Vasco, el Ministerio de Sanidad y Política Social y Red.es para el desarrollo de servicios públicos digitales en el Sistema Nacional de Salud, programa "Sanidad en Línea fase II".
[240] SANZ URETA y HUALDE, "Aspectos Técnicos...", cit., 2000, p. 72.
[241] HERRANZ RODRÍGUEZ, "Aspectos Éticos...", cit., 2000: "El médico optará por usar la telemedicina cuando considere que, en las circunstancias del caso, esa es la mejor opción a su alcance". "Debe preocuparse seriamente el médico de la calidad y buen estado de los instrumentos técnicos que usa",
[242] Artículo 22.1 del Código de Ética y Deontología Médica de 1999, que ciertamente podría entenderse como una auténtica barrera al desarrollo de la telemedicina , pero que aquí se considera simplemente como un llamamiento al buen uso de las TIC por los profesionales sanitarios.
[243] Artículo 14.1 LBAP.
[244] MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 21: "Se pude considerar la Historia Clínica el elemento básico de información para el médico en su práctica diaria".

Para desarrollar las citadas actividades resulta indispensable que la información contenida en las historias clínicas fluya de una manera segura, sencilla y rápida. En este sentido, la informatización de la historia clínica resulta un paso necesario en la creación de ese flujo. Este proceso de incorporación de la telemática al ámbito sanitario se está consolidando a día de hoy en las sociedades tecnológicamente más avanzadas. No ha sido, ni mucho menos, un ejercicio sencillo y a pesar de sus evidentes ventajas, la informatización de la historia ha sido un proceso largo y lento[245]. Se han señalado como principales motivos de esta circunstancia la escasa voluntad política que hasta ahora ha mostrado la clase dirigente[246] y la inicial falta de interés o desconfianza de los médicos hacia esta herramienta[247]. A pesar de todo, en los últimos años parece que el proceso de mecanización se ha acelerado y que la mayoría de sistemas sanitarios lo han asumido como un proyecto imprescindible[248].

Cuando se habla de la informatización de las historias cínicas hay que tener en cuenta que entre la clásica historia en formato papel y la historia de salud electrónica hay distintos estadios. Algún autor se refiere a estas distintas fases descritas con acierto por la *Medical Records Institute.* En primer lugar se encuentra la "historia clínica con informatización", en la que se mantiene aún un amplio contenido en papel y en el que el tratamiento informatizado es muy limitado, centrado prioritariamente en elementos administrativos. En una segunda fase se situaría la "historia clínica digital", en la que la información se digitaliza mediante *scanner* pudiendo manipular estos documentos desde el ordenador, pero como si fueran imágenes. La "historia clínica Electrónica" constituirá el tercer eslabón y se caracteriza por la infraestructura para introducir, procesar y almacenar la información, porque la información se adapta a las posibilidades del ordenador integrándose con aplicaciones y bases de datos interrelacionadas, sin mantener la estructura del formato de papel; y porque el almacenaje deja de ser pasivo, permitiendo ayudas interactivas. En cuarto lugar estaría la "historia clínica basada en ordenadores", que tendría como característica principal la interoperabilidad entre los sistemas de información de los centros sanitarios y sus bases de datos, tanto a nivel nacional como internacional. Y por último, se encontraría la historia de salud electrónica[249], que añade al nivel anterior el que al historial se incluya cualquier información relativa a la salud de un individuo, no

[245] GOST GARDE, "Gestión Sanitaria...", cit., 2000, p. 44.
[246] "Sólo se requiere un poco de interés político", Diario Médico, 26 enero 2004, en http://www.diariomedico.com/.
[247] A fecha de 2003 tan sólo "entre un 5 o 10 por ciento de los médicos utilizan la Historia Clínica Electrónica como una herramienta más de trabajo", *Diario Médico*, 12 diciembre 2003. Sin embargo, tampoco es justo achacar a los médicos la totalidad de la culpa por la lentitud en el avance del proceso, ya que lo cierto es que las inversiones en la formación y motivación de éstos ha sido mínima. Hasta ahora, las políticas en este ámbito se han centrado sobre todo en el desarrollo tecnológico, dejando a un lado el aspecto humano, sin tener en cuenta que "los sistemas de información dependen de las personas que lo forman. Los ordenadores que se utilizan para trasladar la información son meros instrumentos", Diario Médico, 18 junio 2003, en http://www.diariomedico.com/.
[248] MARIMÓN, *La Sanidad...,* cit., 1999, p. 325, "la mejor medida para evaluar un sistema de información en el sector sanitario es su nivel de Historia Clínica. El hecho de que las Historias Clínicas estén basadas en papel o en formatos y soportes electrónicos representa una diferencia cualitativo importante"; FERNÁNDEZ HIERRO, "Régimen jurídico general…", cit., 2002, p. 172.
[249] ESCOLAR CASTELLÓN, IRABURU ELIZONDO, y MANSO MONTES, "Modelos de Historia...", cit., 2003, p. 121: Con el concepto Historia de Salud se hace referencia a un concepto mucho más amplio que el de la HC, y "que podemos definir como el registro longitudinal de todos los eventos de una persona relativos a su salud tanto preventivos como asistenciales (desde el nacimiento hasta su fallecimiento), incluyendo la historia de asistencia primaria y de todos los episodios puntuales de la asistencia especializada, es decir la Historia Clínica clásica estaría incluída en la Historia de Salud".

sólo la generada en la interacción con el sistema sanitario, a saber: información de tipo social, hábitos de salud, empleo de medicinas y terapias, etc., y que el propio individuo coopera en su historial[250]. Se ha llegado a plantear incluso que en última instancia el concepto de historia clínica debe desaparecer para "dar paso a un enfoque de <<conjunto organizado y estructurado de información clínica del paciente>> que presente una visión de continuidad y de cohesión"[251].

De forma paralela al proceso de informatización de las historias clínicas se ha planteado en el ámbito sanitario un debate de interés relacionado con la estructura que ha de tener el sistema de información a emplear. Se hace referencia a si la historia clínica ha de estar centralizada o distribuida[252]. El sistema centralizado consta de una computadora principal a la que se conectan las demás terminales y en la que la información, su procesamiento y control, y el servicio están centralizados, mientras que en el distribuido hay distintas entidades autónomas interconectadas[253]. Hoy día parece que la tendencia es la de la integración de la información sanitaria[254] y la creación de la historia clínica única, no tanto a nivel de centro, sino a nivel de todo un sistema sanitario, que tiene también, como se irá viendo, respaldo legal.

Las ventajas de la historia de salud electrónica con respecto a la historia clínica en formato de papel son múltiples y prácticamente nadie cuestiona las posibilidades que la primera ofrece[255]. Posiblemente las únicas ventajas que el papel presenta frente a la historia de salud electrónica sean la movilidad física del documento y la facilidad que da la redacción a mano[256]. Sin embargo, frente a estos escasos aspectos positivos, las contras son varias: la historia tradicional es utilizable en un solo lugar físico; el riesgo de que se pierda es alto; muchas veces aparece incompleta y se separan los documentos en base a las distintas necesidades de los distintos profesionales; muchas veces es ilegible al estar redactada a mano; hay mayor riesgo de que se produzcan errores; muchas veces no se firma ni se fija la fecha y la hora; gran riesgo de que aparezca información duplicada e innecesaria; una misma historia puede quedar organizada de distintas maneras dependiendo de la necesidad de los distintos profesionales, lo que lleva a la desorganización de la información que tiene como consecuencia que su manipulación sea menos sencilla; el riesgo de que el contenido se vea alterado es también mayor pues los mecanismos de control son menores; la protección de la confidencialidad es menor pues los sistemas de seguridad son también menores; el riesgo de que el soporte se deteriore es mayor, los problemas

[250] MARIMÓN, *La Sanidad...,* cit., 1999, pp. 331-333.
[251] REIGOSA, CASTILLA y BLANCO, "Desde la informática...", cit., 2002, p. 189; IBÁÑEZ FRAILE, "Historia clínica…", cit., 2003, p. 205.
[252] SÁNCHEZ-CARO, "El uso y acceso a la historia…", cit., 2010, p. 1.062.
[253] CRESPO, MALDONADO, ROBLES y CHAVARRÍA, "Tecnologías de la Información...", cit., 2003, p. 149; ARTAL, "La informatización…", cit., 2006, p. 116-117, pone de manifiesto la necesidad de que las bases de datos estén, cuando menos, intercomunicadas, independientemente se trate de historias clínicas únicas o no.
[254] LÓPEZ CARMONA, "e-Salud, Confidencialidad…", cit., 2006, p. 97.
[255] ESCOLAR, "La inferencia...", cit*.,* 2003, p. 287, para ver un estudio completo a este respecto, donde se exponen con más rigor las aportaciones de esta herramienta en tres niveles: el vegetativo (consecuencia de la aplicación de la tecnología de una forma automática), operativo (cuando esta tecnología la aplicamos a desarrollos específicos para resolver problemas reales relacionados con las salud), y epistemológico o del conocimiento (cuando las aplicaciones específicas no tratan de resolver un problema real directamente, si no que están realizadas con el fin de incrementar o tratar con el conocimiento); SÁNCHEZ-CARO, "El uso y acceso a la historia…", cit., 2010, p. 1.061.
[256] ESCOLAR CASTELLÓN, IRABURU ELIZONDO, y MANSO MONTES, "Modelos de Historia...", cit., 2003, p. 139.

de almacenaje son obvios; las posibilidades de que los datos se puedan separar en base a las necesidades de los profesionales son mínimas[257].

Frente a las limitaciones de la historia clínica en formato de papel, la historia de salud electrónica presenta ventajas que se podrían resumir en las siguientes: la capacidad de almacenaje de información que tienen los ordenadores, hace que la informatización de la historia conlleve la liberalización de espacio en los centros[258]; se garantiza la legibilidad de los documentos; la alterabilidad se reduce, y en todo caso las modificaciones, su fecha y autor, quedan registradas[259]; se evitan las pérdidas físicas de las historias; se reduce el riesgo de pérdida de documentos en caso de accidentes, mediante copias de seguridad y mecanismos en espejo; se minimiza la posibilidad de que se realicen errores[260]; la información queda ordenada atendiendo a las necesidades de los distintos profesionales[261]; la disponibilidad será total pudiendo acceder en cualquier momento y en cualquier lugar; se garantiza la confidencialidad en el sentido establecido en la LOPD con la posibilidad de establecer niveles de acceso a la información[262]; la informatización del soporte, y en especial internet permitirá la integridad de la información en una única historia de salud[263]; evita duplicidades y estudios complementarios; ahorra tiempo a pacientes, profesionales sanitarios, una vez formados[264], y al personal administrativo[265]; facilita el análisis, la explotación, codificación y gestión de los datos[266]; permite

[257] FALAGÁN y NOGUEIRA, "La información...", cit., 2003, p. 90.

[258] MAZÓN RAMOS y CARNICERO GÍMENEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 24: "Los sobres (que contienen las Historias Clínicas en formato papel) (...), deben ser almacenados en archivos de cada vez mayor tamaño, que ocupan un espacio precioso en los centros sanitarios y con mucha frecuencia acaban en naves situadas en polígonos industriales alejados de los centros hospitalarios. Además del probelema de almacenamiento se añade entonces el de transporte, lo que hace que las historias no siempre están accesibles cuando son necesarias"; MORENO VERNIS, "Documentación Clínica…", cit., 2002, p. 48.

[259] En la medida en que se controla el acceso a la información, se reduce su alterabilidad, y en todo caso, toda modificación queda registrada y controlada, siempre, claro está, que las medidas de seguridad sean relamente eficaces.

[260] En la medida en que el propio paciente tiene acceso a la historia y puede corregir incongruencias, y en que la información aparece integrada evitando las islas, los errores se reducen.

[261] La telemática permite que las informaciones se estructuren de distinta forma para que puedan atender a necesidades y circunstancias concretas: casos de urgencia, casos de enfermedades crónias, etc. REIGOSA, CASTILLA y BLANCO, "Desde la Informática...", cit., 2002, p. 187: "Las necesidades no son las mismas en las diferentes situaciones que se producen en un centro (consultas, urgencias, hospitalización, etc."
"Cada momento requiere que el sistema elija, con la menor interacción de usuario y de forma efectiva, la información que debe presentar y que debe destacar, sin detrimento de que toda la información del paciente esté siempre accesible si el usuario dispone del privilegio para ello".

[262] MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 25: "La Historia Clínica en soporte informático permite diferenciar sus contenidos de forma que se pueda acceder a toda o a parte de la información, según los privilegios de acceso que tengan los empleados del centro",

[263] La posibilidad de que toda la información relativa a la salud de un mismo paciente, independientemente de la fuente, aparezca en un único documento, supone uno de los principales avances de la informatización de la HC, pues facilita el que dicha información sea actual y completa. MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 25: "La mayor ventaja desde el punto de vista clínico es que la historia clínica informatizada puede ser única para cada paciente recogiendo toda la información relativa al mismo".

[264] Gracias por ejemplo a la "disponibilidad de los resultados en tiempo real para todos los usuarios del programa" lo cual evita retrasos en la toma de decisiones; ESCOLAR, IRABURU y MANSO, "Modelos de Historia...", cit., 2003, p. 135.

[265] MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 25: "La confección de partes médicos de alta y baja, las recetas médicas, los informes, la documentación necesaria en admisión se automatiza. Resulta también mucho más sencilla la revisión de los datos necesaria para controles de calidad, estudios estadísticos y de investigación".

[266] MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 25.

incorporar gráficos e imágenes[267]; hace que sea viable la Tarjeta Sanitaria Inteligente[268] y posibilita la identificación única[269]; posibilita la actualización de la información en tiempo real[270]; hace posible el establecimiento de enlaces, desde la propia historia de salud electrónica, a protocolos de actuación, a informaciones complementarias, a bibliotecas virtuales[271]; etc..

Sin embargo, a pesar de todas las bondades que se han señalado, la historia de salud electrónica también presenta problemas, que se han apuntado al hablar de la telemedicina en general pero que merecen ser subrayados ahora. La mayor dificultad al implantar la historia de salud electrónica, sobre todo a la hora de lograr una completa integración, viene dada por la necesidad de establecer estándares que posibiliten la transmisión de información entre diferentes sistemas, incluso de distintos Estados[272]: estándares en seguridad, en terminología y en comunicación[273], para que los sistemas sean compatibles[274].

Otro de los problemas al que se ha hecho referencia más arriba concierne a los profesionales de la sanidad: la falta de formación, y sobre todo de motivación de éstos podría frenar el desarrollo hacia la historia de salud lectrónica[275]. Por lo demás, los obstáculos que hay que salvar para que este proyecto sea una realidad se refieren sobre todo al coste de la infraestructura, a la necesidad de garantizar en todo caso la confidencialidad de la información que se maneja, y por lo tanto la seguridad, y a la dependencia con las nuevas tecnologías[276].

La consideración de estos factores como ventajas o desventajas ha de relativizarse en la práctica. Si bien es cierto que en general la informatización de la historia clínica plantea posibilidades que han de ser vistas con buenos ojos, no hay que dejar de señalar que estas ventajas sólo podrán hacerse efectivas si la implantación de la telemedicina se realiza atendiendo

[267] La HSE posibilita que al texto se le agregen imágenes en formato de foto o vídeo, lo cual, obviamente, abre la puerta a la práctica de la asistencia a distancia, con la posibilidad de emplear la videoconferencia como medio de comunicación entre médico y paciente.

[268] MAZÓN RAMOS y CARNICERO GIMÉNEZ de AZCÁRATE, "La Informatización...", cit., 2000, p. 25., esta tarjeta "permite que el paciente lleve consigo información clínica relevante, con lo que la tarjeta se convierte en una *tarjeta clínica*", que como afirman ESCOLAR, IRABURU y MANSO, "Modelos de...", cit., 2003, p. 136. "posibilita la consulta de datos desde puntos externos a la red".

[269] IBÁÑEZ FRAILE, "Historia clínica…", cit., 2003, p. 205.

[270] "La HCE, el santo grial del internet médico", *Diario Médico*, 12 diciembre 2003

[271] GOST GARDE, "Gestión Sanitaria...", cit., 2000, p. 45.

[272] En el Estado se ha puesto muchas veces de manifiesto la necesidad de crear estos estándares debido a que cada Comunidad Autónoma está desarrollando su propia iniciativa, por lo que "cabe la duda de que en un futuro esa información pueda distribuirse desde las distintas plataformas", <<La HCE, el santo grial del Internet médico>>*, Diario Médico,* 12 diciembre 2003. De alguna manera, se puede justificar esta situación, señalando que las iniciativas regionales responden a particularidades propias, sin embargo, "si subimos un nivel, al escenario nacional, es necesario que se pacte, ya que, aunque no es necesaria la homogeneidad entre las regiones, sí lo es la compatibilidad", Diario Médico, 18 junio 2003.

[273] FERRER ROCA, *La Telemedicina...*, cit., 2001, p. 91, pone de manifiesto como "en los años 80 y 90 primó la libertad de elección tanto en la demanda como en el suministro, lo que dio lugar a una considerable fragmentación",

[274] GOST GARDE, "Gestión Sanitaria...", 2000, p. 45: "si no se posibilita como compartir información entre diferentes instituciones garantizando simultáneamente la confidencialidad de los datos y la participación activa de los pacientes, la potencialidad de la Historia Clínica Informatizada quedará seriamente mermada". IBÁÑEZ FRAILE, "Historia clínica…", cit., 2003, p. 217.

[275] FALAGÁN y NOGUEIRA, "La Información...", cit., 2003, p. 100, afirman que es necesario, por lo tanto, "encontrar un interfaz lo suficientemente atractivo y amigable para que no produzca rechazos",

[276] MÉJICA GARCÍA, *El Enfermo Transparente…*, cit., 2002, p. 32, pone el acento en la necesidad de garantizar la seguridad, fundamentalmente, a la hora de controlar los accesos a los datos sanitarios.

a las exigencias de la práctica sanitaria. Por ejemplo, desde el punto de vista de la defensa de la confidencialidad y la protección de los datos sanitarios se ha planteado como principal ventaja de la historia clínica electrónica, la posibilidad que ofrece a la hora de controlar los accesos que se producen sobre la documentación sanitaria. Es conocido que no todos los profesionales sanitarios tienen que tener acceso a todas las historias clínicas y a toda la documentación. Por razones obvias no es el mismo el acceso que debe tener un médico de cabecera, que tiene adjudicados unos pacientes determinados, que un especialista, que podrá encontrarse con cualquier paciente. Tampoco es el mismo el trabajo del personal de enfermería. La limitación en el acceso a la documentación sanitaria debe darse atendiendo a la cualidad de quien quiere acceder a la información (no es lo mismo un médico que un enfermero) y al contenido de la información a la que se quiere acceder (es distinta la información a la que ha de acceder un enfermero que un médico). Pues bien, la historia clínica electrónica facilita que el acceso sea limitado, cosa que la historia convencional hacía difícil[277]. La telemática plantea numerosas alternativas para que cada uno de los profesionales tenga acceso exclusivamente a la información estrictamente necesaria para llevar a cabo sus tareas, de manera que los citados derechos queden salvaguardados.

Esta posibilidad que ha sido valorada como una ventaja ha de replantearse, sin embargo, de acuerdo a las exigencias que la realidad de la práctica sanitaria presenta. El acceso limitado podría afectar en la práctica a los posibles tratamientos. Teniendo en cuenta situaciones que se dan en la realidad, establecer un sistema excesivamente rígido de control de accesos puede afectar negativamente a la realización de las tareas sanitarias[278]. Las rotaciones, las guardias, la delegación de funciones, entre otras, hacen que en muchas ocasiones sea complicado crear límites o perfiles de acceso estáticos, pues en la realidad son numorosos los casos en que una persona deba realizar un acceso que en un inicio no le correspondía. Con esto simplemente se quiere decir que estos instrumentos han de ser valorados siempre de acuerdo a las exigencias que la práctica sanitaria conlleva. En el caso de la receta electrónica, por ejemplo, si bien limitar los accesos atendiendo a los perfiles de cada profesional puede resultar complicado, es perfectamente plausible controlar, aunque sea *a posteriori,* los accesos que se han realizado sobre los distintos documentos.

Sea como sea, la apuesta en la actualidad por un sistema avanzado de gestión de historias clínicas es clara. En primer lugar, se tiende a la integración de la información. Las propias leyes recogen el compromiso por la historia clínica única[279]. Se trata de evitar que en un sistema sanitario se dupliquen las informaciones y se creen islas de información, y de crear una única base de datos por cada paciente, independientemente de que la información haya sido recabada de distintas fuentes[280]. Proyectos de centralización como el ya descrito Osabide, aplicado en el

[277] RAMÍREZ NEILA, "Accesos legítimos…", cit., 2009, p. 294.
[278] SÁNCHEZ CARO, "El uso y acceso a la historia…", cit., 2010, p. 1.072.
[279] Artículo 3.b) Decreto 101/2005, 22 de diciembre, por el que se regula la Historia Clínica en Castilla y León: "*Historia clínica única: todos los datos de los contactos asistenciales relacionados por un único número de identificación del paciente*".
[280] DA Única Ley 21/2000, 29 de diciembre, sobre los derechos de información concernientes a la salud y la autonomía del paciente, y la documentación clínica, de Cataluña: "*El Departamento de Sanidad y Seguridad Social, con el objetivo de avanzar en la configuración de una historia clínica única por paciente, debe promover, mediante un*

Sistema Vasco de Salud, no suponen otra cosa que integrar la información sanitaria en una única base de datos a la que los distintos profesionales podrán tener acceso para poder desarrollar la labor que les corresponda. En segundo lugar, la apuesta por la historia clínica electrónica parece también indudable. Ya se ha comentado que para hacer efectiva, entre otras propuestas, la integración de la información, resulta necesaria la aplicación de la telemática a la gestión de las historias clínicas. La relación entre ambos procesos se reconoce también en las leyes[281]. Este tipo de fórmulas requieren de la transmisión constante de datos de un lugar a otro y esto sólo es posible con la aplicación de las TIC. Así, no sólo en los planes y proyectos arriba citados, sino también en las normas se recoge la consolidación de este proyecto[282].

III.3.2. La Tarjeta Sanitaria Inteligente.

Si la historia de salud electrónica constituye el instrumento clave en los Sistemas de Información Sanitaria al ser el documento que fundamentalmente contiene la información relativa a los usuarios del servicio sanitario, la tarjeta sanitaria supone el complemento indispensable para que la manipulación de toda esta información se pueda llevar a cabo con eficacia. Si se entiende que el sistema de salud es una organización dirigida a atender a la ciudadanía en los problemas relativos a la salud, basándose fundamentalmente en la información concerniente a

proceso que garantice la participación de todos los agentes implicados, el estudio de un sistema que, atendiendo a la evolución de los recursos técnicos, posibilite el uso compartido de las historias clínicas entre los centros asistenciales de Cataluña, a fin de que pacientes atendidos en diversos centros no se tengan que someter a exploraciones y procedimientos repetidos, y los servicios asistenciales tengan acceso a toda la información clínica disponible"; Artículo 15.4 LBAP: "*La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial*". Artículo 6.3.1 Resolución 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam, de Castilla la Mancha: "*Cada HC es única y tendrá un número de identificación único para cada paciente del centro. Cuando finalice el proceso de implantación de la HC electrónica ésta será única para cada paciente y para toda la red asistencial del Sescam. En todo caso, la HC recogerá toda la información integrada y acumulativa relativa al curso clínico del paciente*"; Artículo 5 Decreto 101/2005, 22 de diciembre, por el que se regula la Historia Clínica en Castilla y León: "*1. En el ámbito del Sistema de Salud de Castilla y León, la historia clínica será única por paciente. En los centros, servicios y establecimientos sanitarios ajenos al Sistema de Salud de Castilla y León, la historia clínica será única por paciente en cada centro.*
2. La historia clínica deberá encontrarse unificada dentro de un mismo centro, servicio o establecimiento sanitario. Una historia clínica estará unificada cuando todos los documentos activos sustentados bajo un mismo soporte se encuentren archivados en un mismo contenedor".

[281] Exposición de Motivos Decreto 101/2005, 22 de diciembre, por el que se regula la Historia Clínica en Castilla y León: "*La utilización cada vez mayor del as nuevas tecnologías pone a disposición de los centros sanitarios medios electrónicos, informáticos y telemáticos que, aplicados también a la historia clínica, suponen cambios en su configuración. Ello puede contribuir a la implantación de la historia clínica única, no ya en el marco de cada centro o Área de Salud, como propugnaba el derogado artículo 61 de la Ley 14/1986, de 25 de abril (RCL 1986/1316), General de Sanidad, y el artículo 28 de la Ley 1/1993, de 6 de abril (LCyL 1993/132), de Ordenación del Sistema Sanitario de Castilla y León, sino para el conjunto de la Comunidad Autónoma e incluso para el ámbito nacional*".

[282] DA Primera Decreto 101/2005, 22 de diciembre, por el que se regula la Historia Clínica en Castilla y León: "*Con el objetivo de avanzar en la configuración de una historia clínica única por paciente en el ámbito del Sistema de Salud de Castilla y León, la Gerencia Regional de Salud realizará las actuaciones necesarias para informatizar la historia clínica y su acceso a toda la información clínica disponible, sin perjuicio de lo dispuesto en la Disposición Adicional Tercera de la Ley Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica*"; Decreto 29/2009, 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en Galicia; Artículo 6.3.1 Resolución 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam, de Castilla La Mancha.

estos problemas, parece evidente que identificar a cada ciudadano es algo fundamental, mucho más en la actualidad, si se pretende que esta información fluya por las "autopistas de la información" de todo el mundo de forma rápida y constante[283].Tanto es así que el ordenamiento estatal dispone que el acceso a las prestaciones sanitarias se facilitará a través de las tarjetas sanitarias, en la medida en que se trata del documento que refleja la identidad de los sujetos que tienen acreditado el derecho a recibir asistencia sanitaria pública[284].

Es por esto que hoy día la mayoría de los países de la UE cuentan con tarjetas que cuando menos cumplen este fin[285]. Y se dice cuando menos, porque comienzan a generalizarse las tarjetas electrónicas, que constituyen una llave de acceso a la información sanitaria, y las tarjetas inteligentes, dirigidas a convertirse en soporte de información relativa a la salud de los titulares de dicha herramienta.

Cabe en este momento realizar una básica distinción entre los diferentes tipos de tarjeta existentes: las que simplemente se dirigen a identificar al paciente (las de plástico con caracteres en relieve), las magnéticas (que además de identificar constituyen la llave de acceso a la información del paciente), las tarjetas electrónicas de memoria (almacenan datos pero no contienen microprocesador), y las tarjetas electrónicas inteligentes o *smartcards*[286] (además de almacenar datos, contienen un microprocesador)[287].

En una sociedad como la actual, de la información, en la que se pretende que la información fluya por las redes de todo el globo, el salto a la tarjeta electrónica o magnética en el ámbito sanitario es necesario, pues constituye un instrumento seguro (a traves de herramientas como la firma electrónica) de acceso a la información sanitaria de la ciudadanía. De hecho, hoy día no se cuestiona la utilidad de las tarjetas electrónicas y las principales discusiones están girando en el nivel superior, en torno a las dos últimas modalidades de las citadas tarjetas, por su capacidad para portar información relativa a la salud, sobre todo, en relación a las denominadas tarjetas inteligentes, por la capacidad que tienen de procesar esta información[288].

---

[283] CARNICERO y VÁZQUEZ, "La identificación...", cit., 2003, p. 110: "El intercambio de información electrónica exige la certeza de la identidad del paciente". En un sistema en el que la información se va a manejar desde distintos lugares en momentos diferentes, la identificación es fundamental.

[284] Artículo 57 Ley 16/2003, 28 de mayo de 2003, de cohesión y calidad del Sistema Nacional de Salud. Artículo 2 RD 183/2004, 30 de enero 2004, por el que se regula la tarjeta sanitaria individual: "*1. Las Administraciones sanitarias autonómicas y el Instituto Nacional de Gestión Sanitaria emitirán una tarjeta individual con soporte informático a las personas residentes en su ámbito territorial que tengan acreditado el derecho a la asistencia sanitaria pública*".

[285] Comunicación de la Comisión Europea relativa a la introducción de la Tarjeta Sanitaria Europea, COM (2003)73 final, del 17/02/03, en la que se hace un análisis detallado de los distintos modelos de Tarjeta Sanitaria que se emplea en los diferentes países de la Unión.

[286] ZOREDA, ICHASO, y COBIÁN, "Modelo de Tarjeta...", cit., 1991. Las *memory cards* no disponen de capacidad de proceso, pero en todo caso, tanto éstas como las *smart cards* pueden incorporar dos tipos de memoria: "memoria no borrable, se trata de tarjetas con una memoria de las denominadas ROM o EPROM (de sólo lectura)" y "memoria borrable o actualizable (...) se pueden almacenar datos, actualizarlos e incluso borrarlos".

[287] MARIMÓN, *La Sanidad...*, cit., 1999, p. 288. Este autor incluye otro tipo de Tarjetas, las Ópticas, si bien hoy día la principal discusión sobre las Tarjetas Sanitarias parece girar en torno a las Tarjetas Electrónicas e Inteligentes; MÉJICA GARCÍA, *El Enfermo Transparente...,* cit., 2002, p. 25.

[288] LÓPEZ CARMONA, "E-salud, Confidencialidad...", cit., 2004. Existen en la actualidad dos tendencias que dirigen el desarrollo de las Tarjetas Sanitarias. La primera se basa en un sistema en el que la información se encuentra en la red y el ciudadano simplemente tiene que identificarse para que la dicha información sea accesible. Mientras tanto, la

Tras su nacimiento a comienzos de la década de los 70[289], la tarjeta inteligente se ha ido desarrollando hasta hoy[290], momento en el que su uso se está expandiendo tanto en el sector sanitario como en otros como el bancario. Las posibilidades que ofrecen estas tarjetas para poder trabajar sobre la información que en éllas se contiene hace que su empleo pueda ser muy útil para supuestos en que el acceso a la historia de salud electrónica en red sea verdaderamente dificultosa, como en los casos de urgencia en la calle[291] o en el domicilio[292]. Ciertamente, la necesidad de implantar estas tarjetas puede estar justificada para estos supuestos limitados. Por lo demás, en el concreto ámbito de la sanidad, en los casos, por ejemplo, en que el paciente se encuentra en un centro hospitalario, bastaría con una tarjeta electrónica o magnética que identificase al paciente y diese acceso rápido y seguro a una historia completa y actualizada.

La creación de este tipo de tarjetas se ha ido generalizando en todos los ámbitos territoriales. En la CAPV, en el marco del Plan Euskadi en la Sociedad de la Información, se ha creado una Tarjeta Sanitaria Ciudadana Electrónica que garantiza la identificación de los usuarios y constituye el eslabón de enlace entre la ciudadanía y su historia clínica posibilitando el acceso a su información y su manipulación[293]. Se pretende que la Tarjeta Sanitaria Electrónica se convierta en la herramienta que posibilite una relación telemática segura de los ciudadanos con la Administración Sanitaria[294]. Recientemente, este proyecto se ha traducido en la creación de la Tarjeta ONA (Tarjeta Sanitaria Electrónica con Usos Ciudadanos/Osasen eta Nortasun Agiria), que constituye una herramienta con la que cuentan los ciudadanos que así lo han solicitado[295]. En cualquier caso, la apuesta en el ámbito autonómico por la tarjeta sanitaria electrónica es clara y se recoge, también, en las normas[296].

---

segunda tendencia se fundamenta en la idea de que es el propio ciudadano el que lleva la información incorporada en su tarjeta equipada con un chip.

[289] LÓPEZ CARMONA, "E-Salud, Confidencialidad...", cit., 2004.

[290] MARIMÓN, *La Sanidad...,* 1999, p. 289, destaca el hecho de que en la actualidad "decenas de miles de personas están trabajando en el mundo en el progreso de las Tarjetas Inteligentes, en particular en temas de seguridad".

[291] ZOREDA BARTOLOME, SÁNCHEZ FREIRE, REDONDO FDEZ.-REBOLLOS., SÁNCHEZ REILLO y DE PEREDA HUELVES, "Tarjeta Sanitaria...", cit., 1997.

[292] ZOREDA, ICHASO, y COBIÁN, "Modelo de Tarjeta...", cit., 1991: "Incluso en el caso de existir una competa y eficaz red entre centros", que es el objetivo de la eSalud, "el paciente tendría que seguir siendo portador de información, como es el caso de la atención domiciliaria".

[293]http:// www.euskadi.net/eeuskadi/

[294] Exposición de Motivos de la Orden de 22 de noviembre de 2004, del Consejero de Sanidad por la que se establecen Normas sobre el Uso de la Firma Electrónica en las Relaciones por Medios Electrónicos, Informáticos y Telemáticos con el Sistema Sanitario de Euskadi, B.O.P.V., 26 de noviembre de 2004, nº 2004227: "*se establece como una línea de acción preferente la implantación de una Tarjeta Sanitaria que posibilite articular las relaciones con la Administracione Sanitaria incorporando un sistema de certificación que permita la identificación y unas transacciones seguras así como nuevas facilidades de relación*".

[295] http://www.euskadi.net/r33-ona2/es/. Resolución 1/2008, de 14 de enero, del Director de la Secretaría del Gobierno y de Relaciones con el Parlamento, por la que se dispone la publicación de los Convenios celebrados por el Gobierno Vasco, que se indican: Convenio de colaboración con la sociedad Ziurtapen eta Zerbitzu enpresa-Empresa de Certificación y Servicios, Izenpe, S.A. para promover la utilización de tarjetas electrónicas en las relaciones de la ciudadanía con las Administraciones Públicas Vascas.

[296] Artículo 10.1 Decreto 579/2009, 3 de noviembre, por el que se establece la estructura orgánica y funcional del Departamento de Sanidad y Consumo, de Euskadi: "*La Dirección de Aseguramiento y Contratación Sanitaria, además de las que con carácter general se establecen en el artículo 5 de este Decreto, realizará las siguientes funciones: a) La definición y gestión de las especificicaciones de la tarjeta individual sanitaria, como documento acreditativo del aseguramiento pública; así como, su adecuación y desarrollo a la tarjeta sanitaria electrónica, como sistema seguro de relación electrónica entre la Administración sanitaria y la ciudadanía*".

En el ámbito estatal, el objetivo es crear una Tarjeta Sanitaria Única para todo el Estado, que sustituya a las distintas tarjetas de las diferentes CC.AA y que permita la movilidad por todo el territorio estatal[297]. Para ello se pretende que en cualquier parte del Estado se pueda "identificar de forma segura y unívoca a cada ciudadano"[298], mediante la integración de las distintas bases de datos de las CC.AA en una nueva base de datos, dentro del nuevo sistema de alcance estatal, que acredite, mediante dicha identificación, el derecho a recibir asistencia de ese sujeto determinado[299]. Se pretende que con esta identificación segura la tarjeta dé acceso a la información clínica del paciente, independientemente del lugar en el que se encuentre[300] "posibilitando el intercambio de dicha información dentro del Sistema Nacional de Salud en las condiciones legalmente permitidas y siempre con la finalidad de contribuir a la mejora de la calidad asistencial"[301]. El objetivo final es dar una asistencia sanitaria óptima en cualquier lugar del Estado y en cualquier momento, para lo cual hace falta que la información pueda llegar de forma rápida y completa, y sobre todo inequívocamente relacionada al sujeto determinado. Las leyes hoy día vigentes fijan la necesidad de crear tarjetas sanitarias que posibiliten la asistencia sanitaria en cualquier punto del Estado. De esta manera, se obliga a crear tarjetas compatibles con los sistemas del sistema nacional de salud y de las demás comunidades autónomas, y también con los criterios marcados desde la UE[302].

---

[297] "El Gobierno aprueba una Tarjeta Sanitaria Individual válida para todas las Comunidades Autónomas", 02/02/04, Jano *on-line*, en http://db.doyma.es/

[298] Exposición de Motivos RD183/2004 de 30 de enero, que regula la Tarjeta Sanitaria Individual.

[299] Artículo 5.2. del RD 183/2004 de 30 de enero, por el que se regula la Tarjeta Sanitaria Individual: "*Para facilitar la gestión de la población protegida, su movilidad y el acceso a los servicios sanitarios, dicha base actuará como un sistema de intercambio de información entre las Administraciones sanitarias. La información que recoja deberá posibilitar la coherencia de los datos de aseguramiento, evitar la adscripción simultánea a distintos servicios de salud y obtener la mayor rentabilidad posible en los cruces de datos entre los ficheros oficiales necesarios para su correcto mantenimiento*".

[300] "Así, el objetivo de la tarjeta es lograr una identificación "única e inequívoca" de cada persona de tal modo que, "viva donde viva, o transite por donde transite dentro del sistema", su información clínica "pueda ser fácilmente encontrada y utilizada por los profesionales sanitarios, siempre que sea necesario en beneficio de su salud", "El Gobierno anuncia que la Tarjeta Sanitaria Individual se implantará en el plazo máximo de dos años", en Jano *on-line,* 17/07/2003, http://www.doyma.es/.

[301] Exposición de Motivos del RD 183/2004 de 30 de enero, reguladora de la Tarjeta Sanitaria Individual.

[302] Artículo 57 Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: "*1. El acceso de los ciudadanos a las prestaciones de la atención sanitaria que proporciona el Sistema Nacional de Salud se facilitará a través de la tarjeta sanitaria individual, como documento administrativo que acredita determinados datos de su titular, a los que se refiere el apartado siguiente. La tarjeta sanitaria individual atenderá a los criterios establecidos con carácter general en la Unión Europea.*

2. Sin perjuicio de su gestión en el ámbito territorial respectivo por cada comunidad autónoma y de la gestión unitaria que corresponda a otras Administraciones públicas en razón de determinados colectivos, las tarjetas incluirán, de manera normalizada, los datos básicos de identificación del titular de la tarjeta, del derecho que le asiste en relación con la prestación farmacéutica y del servicio de salud o entidad responsable de la asistencia sanitaria. Los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten deberán permitir que la lectura y comprobación de los datos sea técnicamente posible en todo el territorio del Estado y para todas las Administraciones públicas. Para ello, el Ministerio de Sanidad y Consumo, en colaboración con las comunidades autónomas y demás Administraciones públicas competentes, establecerá los requisitos y los estándares necesarios.

3. Con el objetivo de poder generar el código de identificación personal único, el Ministerio de Sanidad y Consumo desarrollará una base de datos que recoja la información básica de asegurados del Sistema Nacional de Salud, de tal manera que los servicios de salud dispongan de un servicio de intercambio de información sobre la población protegida, mantenido y actualizado por los propios integrantes del sistema. Este servicio de intercambio permitirá la depuración de titulares de tarjetas.

En el ámbito europeo el proyecto es similar. A partir del Consejo Europeo de Barcelona[303] se ha apostado por una tarjeta electrónica que posibilite la identificación de un sujeto en cualquier centro del territorio europeo y que garantice la existencia del derecho del mismo a la asistencia sanitaria. Se trata de abandonar los formularios E 110, E 111, E 119 y E128, que en la actualidad se emplean para asegurar esos aspectos. Hoy día, y a partir de 2006, se puede solicitar en cualquier dependencia de la Seguridad Social la Tarjeta Sanitaria Europea, que no es más que una tarjeta identificativa para tener acceso a tratamiento sanitario en cualquier punto de la UE[304].

En un principio, parece que tanto en el ámbito europeo como en el estatal la tarjeta se va a limitar a la identificación de los sujetos como titulares del derecho a la asistencia en el territorio europeo y a facilitar el acceso a su información clínica. Sin embargo, como se decía anteriormente, no parece que vaya a pasar demasiado tiempo antes de que dichas tarjetas informatizadas se empleen como soportes de la información relativa a la salud de las personas convertidas en tarjetas sanitarias inteligentes. Es más, si se atiende a la Comunicación de la Comisión relativa a la introducción de la tarjeta sanitaria europea, se observará que lo que se pretende en última instancia es eso mismo, implantar una tarjeta sanitaria inteligente: "se podría estudiar también la posibilidad de integrar en la tarjeta europea algunas funcionalidades relacionadas con la salud del interesado, por ejemplo el acceso a datos médico útiles para dispensar asistencia médica de urgencia o a información relativa a los tratamientos recibidos por el asegurado"[305].

Las críticas a esta posibilidad no han tardado en llegar. Tanto la Agencia de Protección de Datos (APD)[306], como la Sociedad Española de Medicina Familiar y Comunitaria (semFYC), como la Organización Médica Colegial (OMC)[307], han planteado serias dudas sobre la legalidad de la posibilidad de que la tarjeta sanitaria incorpore información relativa a la salud de los ciudadanos.

---

4. Conforme se vaya disponiendo de sistemas electrónicos de tratamiento de la información clínica, la tarjeta sanitaria individual deberá posibilitar el acceso a aquélla de los profesionales debidamente autorizados, con la finalidad de colaborar a la mejora de la calidad y continuidad asistenciales.

5. Las tarjetas sanitarias individuales deberán adaptarse, en su caso, a la normalización que pueda establecerse para el conjunto de las Administraciones públicas y en el seno de la Unión Europea".

[303] Conclusiones de la Presidencia. Consejo Europeo de Barcelona, 15-16 de marzo de 2002.

[304] http://:ec.europa.eu/ Decisión nº 189 de la Comisión Administrativa para la Seguridad Social de los Trabajadores Migrantes (CASSTM) de 18 de junio de 2003, dirigida a sustituir por una tarjeta sanitaria europea los formularios necesarios para la aplicación de los Reglamentos (CEE) nº 1408/71 y (CEE) nº 574/72 del Consejo en lo que respecta al acceso a la asistencia sanitaria durante una estancia temporal en un Estado miembro distinto del Estado competente o de residencia; Decisión nº 190 de la CASSTM de 18 de junio de 2003, relativa a las características técnicas de la tarjeta sanitaria europea; Decisión nº 191 de la CASSTIM de 18 de junio de 2003, relativa a la sustitución de los formularios E 111 y E 111B por la tarjeta sanitaria europea.

[305] COM (2003) 73 final. DA Única RD 183/2004 de 30 de enero, por el que se regula la Tarjeta Sanitaria Individual: "*En la medida en que se establezcan por la Unión Europea criterios de normalizción que faciliten la circulación y mejora de la asistencia sanitaria de pacientes en el ámbito comunitario, las tarjetas sanitarias individuales del Sistema Naciona de Salud deberán adaptarse a aquéllos*"

[306] "La Agencia de Protección de Datos detecta problemas en la seguridad de la futura Tarjeta Sanitaria", en Jano on-line, 10/02/2003, en http://www.doyma.es/.

[307] "La semFYC pide garantías para que el paciente controle el acceso a su historial con la tarjeta sannitaria",Jano on-line, 16/01/2003, en http://www.doyma.es/.

Ciertamente, las tarjetas inteligentes y las *memory-cards,* en cuanto incorporan información relativa a la salud de las personas, crean cierta incertidumbre sobre su capacidad para garantizar la confidencialidad de la información que contienen. Es evidente que las nuevas tarjetas, por el hecho de convertirse en soporte de informacion tan relevante como la sanitaria, plantean más riesgos que las tradicionales tarjetas sanitarias o cartillas, que no contienen tal información, sin embargo, en la actualidad la seguridad, desde el punto de vista técnico, está garantizada en niveles más o menos aceptables. El verdadero problema viene del ámbito jurídico. Es necesario establecer un marco normativo que determine qué información pueden contener esas nuevas tarjetas, la finalidad con que se puede emplear la misma, quiénes pueden tener acceso a dicha información, etc.[308]. Si se realiza la necesaria inversión para establecer las mínimas condiciones de seguridad técnica, y, a su vez, se fija un marco jurídico que determine con claridad el uso que se pueda dar a dichas tarjetas, teniendo siempre en consideración el derecho a la autodeterminación informativa de los ciudadanos, las tarjetas inteligentes pueden ser instrumentos verdaderamente útiles.

III.3.3. La Receta Electrónica.

La receta electrónica es otro de los grandes proyectos en la aplicación de las TIC al ámbito sanitario. En los casos en que la dispensación de los medicamentos necesita de la intervención del médico, la receta constituye la prescripción del facultativo en la que se le indica al farmaceútico el medicamento y la dosis que ha de tomar un paciente determinado[309]. Se trata, en lo que aquí interesa, por una parte, de un documento a través del cual culmina la asistencia médica[310], y, por otra, de un soporte en el que se integra información relativa a la salud de un individuo determinado. Este instrumento ha sido incorporado tanto en el ámbito autónomico como estatal por diversas normas[311].

[308] Probablemente, la mayor duda reside en saber si será necesario o no el consentimiento del paciente para acceder a la información del paciente.

[309] Artículo 1.a) RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación: "*Receta médica: la receta médica es el documento de carácter sanitario, normalizado y obligatorio mediante el cual los médicos, odontólogos o podólogos, legalmente facultados para ello, y en el ámbito de sus competencias respectivas, prescriben a los pacientes los medicamentos o productos sanitarios sujetos a prescripción médica, para su dispensación por un farmacéutico o bajo su supervisión, en las oficinas de farmacia y botiquines dependientes de las mismas o, conforme a lo previsto en la legislación vigente, en otros establecimientos sanitarios, unidades asistenciales o servicios farmacéuticos de estructuras de atención primaria, debidamente autorizados para la dispensación de medicamentos*".

[310] ACUÑA, "Receta electrónica...", cit., 2002.

[311] Así, en la citada Orden de 22 de noviembre de 2004, del Consejero de Sanidad por la que se establecen Normas sobre el Uso de la Firma Electrónica en las Relaciones por Medios Electrónicos, Informaticos y Telemáticos con el Sistema de Sanitario de Euskadi, se recoge ya, si bien todavía para un área concreta de la CAPV la receta electrónica como sistema de dispensación de medicamentos; Decreto 181/2007, 19 de junio, por el que se regula la receta médica electrónica, de la Comunidad Auónoma de Andalucía; Decreto 159/2007, de 24 de julio, por el que se regula la Receta Electrónica y la Tramitación Telemática de la Prestación Farmacéutica a cargo del Servicio Catalán de Salud, reformado por el Decreto 91/2009, 9 de junio, por el que se modifica la letra h) del artículo 2 del Decreto 159/2007, de 24 de julio, y desarrollado por la Orden SLT/72/2008, 12 de febrero, por la que se desarrolla el Decreto 159/2007, de 24 de julio; Decreto 93/2009, 24 de abril, por el que se regula la Implantación de la Receta Electrónica en el Ámbito del Sistema Sanitario Público de Extremadura; Decreto 206/2008, 28 de agosto, de Receta Electrónica de Galicia; RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación.

Cuando se hace referencia a la receta electrónica se habla de la aplicación de la telemática a este proceso[312]. Ha subrayado la doctrina que lo característico de la receta electrónica es que la receta "no tiene por qué imprimirse en un papel (lo que no quiere decir que no se imprima como comprobante para el paciente)"[313]. Se supone que con este proyecto el médico prescribirá la receta a través del ordenador, ésta irá a una base de datos a la que estará conectado el farmaceútico, quien tendrá acceso a la misma a través de la Tarjeta Sanitaria Electrónica o magnética del paciente[314].

La primera ventaja reseñable de la receta electrónica es que con ella desaparecerá el clásico problema de legibilidad de las recetas. Por otro lado, hará el trabajo de todos los implicados más

[312] FERNÁNDEZ-LLIMOS, "La receta...", cit., diferencia acertadamente la receta eletrónica de otras figuras que muchas veces se confunden entre sí. "La prescipción mecanizada: (...) consiste en la aplicación de un elemento mecánico que escriba la receta, que puede ser desde una impresora, hasta una simple máquina de escribir." "La prescripción informatizada es la que se realiza utilizando un ordenador que revise en una base de datos el producto que desea el prescriptor". "La prescripción asistida por ordenador es el paso siguiente de avance tecnológico en el proceso de prescripción. En éste, el prescriptor tiene al alcance de su ordenador, no sólo una base de datos con los nombres de las especialidades disponibles, sino otros datos sobre éstas, y muy probablemente, sobre el paciente. Es decir, el médico ouede consultar información sobre el medicamento que prescribe y sobre el paciente al que prescribe para, con su juicio clínico, realizar un mejor acto médico".
"Todos ellos son sistemas donde el producto obtenido es una receta tradicional (un P1)".

[313] FERNÁNDEZ-LLIMOS, "La receta...".

[314] CORDOBÉS, "Informática. Receta... (I)", cit., 2001. Decreto 181/2007, 19 de junio, por el que se Regula la Receta Médica Electrónica, en la Comunidad Autónoma de Andalucía, en el que se fija el funcionamiento de esta herramienta: Artículo 5: "*1. En la receta médica electrónica sólo pdorán prescribirse medicamentos o productos sanitarios cuando se inserte la tarjeta sanitaria del paciente y ésta sea validada por el propio sistema informático.*
3. Los medicamentos o productos sanitarios prescritos a un paciente en soporte informático en el mismo acto clínico, se consignarán a su vez en la hoja de instrucciones para el paciente prevista en el artículo 7 del presente Decreto".
Artículo 7: *"1. Cuando la prescripción de la prestación farmacéutica del Sistema Sanitario Público de Andalucía se realice a través de la receta médica electrónica, se imprimirá una hoja de instrucciones, conforme al modelo establecido en el Anexo del presente Decreto, que necesariamente deberá ser entregada al paciente. En esta hoja deben cumplimentarse todos los datos de consignación obligatoria del artículo 3, así como, en el espacio reservado al efecto, las instrucciones del prescriptor que ha de seguir el paciente para un mejor tratamiento y un uso racional del medicamento.*
2. La hoja de instrucciones será firmada en todo caso por el profesional que haya realizado la prescripción".
Artículo 8: *"1. La dispensación sólo podrá ser realizada a través de la conexión telemática con el propio sistema informático. Dicha conexión sólo podrá realizarse desde una oficina de farmacia, cuyo titular cuente con la correspondiente tarjeta de identificación y acceso al sistema informático. DIcha tarjeta será expedida por el órgano administrativo competente en materia de gestión de la prestación farmacéutica.*
2. Salvo en los casos previstos en la disposición transitoria única del presente Decreto, sólo se permitirá el acceso de los profesionales de la oficina de la farmacia al sistema informático si se tiene insertada la tarjeta sanitaria del paciente y ésta es reconocida y validada por el mismo.
6. En el acto de la dispensación se registrarán los datos de consignación obligatoria correspondientes a la dispensación efectuada que serán los siguientes: a) Identificación del medicamento o producto sanitario y su cantidad; b) Número de identificación de la dispensación generado por el sistema informático, que será único e irrepetible; c) Identificación del Código de Identificación FIscal o Número de Identificación del Colegiado de la oficina de farmacia; d) Fecha de dispensación.
7. En el acto de dispensación se imprimirá un justificante de la misma, en el que se incluirán los datos de identificación del titular o titulares de la oficina de farmacia que realiza la dispensación, el número de identificación de la prescripción y de la dispensación, fecha de esta última y se adherirá el cupón o cupones precinto correspondientes. Dicho justificante estará a disposición del órgano competente en la gestión de la prestación farmacéutica del Sistema Sanitario Público de Andalucía.
8. Tras la dispensación correspondiente, la oficina de farmacia estará obligada a devolver la tarjeta sanitaria al paciente, quedando prohibida su retención en dicha oficina de farmacia".

cómodo y sencillo al automatizar el proceso[315]. Otro de los principales avances que aportará la receta electrónica es el hecho de que facilitará el control del gasto y la gestión[316]. Otra ventaja es la reducción de errores en la dispensación y prescripción de medicamentos[317]. Sin embargo, cabe subrayar como mayor logro de esta herramienta la integración del farmaceútico en el proceso asistencial. Con el empleo de las TIC el farmaceútico puede tener acceso a una información más completa del paciente, a las alergias, por ejemplo, o a la evolución farmacoterapéutica del paciente, lo cual ayudará a este profesional a la hora de ver si la prescripción es correcta o puede, en caso de tener dudas o necesitar aclaraciones, comunicarse con el propio médico[318].

Por el contrario, la principal desventaja en la aplicación de la receta electrónica se refiere al importante coste que le supondrá al farmaceútico la adquisición del equipamiento y la formación para su empleo, que además deberá estar en continua actualización[319]. A este problema hay que sumarle otro en el Estado, que ya se ha apuntado más arriba. Se trata de la posible incopatibilidad de los distintos proyectos de las CC.AA, hecho que podría afectar a la movilidad de los ciudadanos[320].

Para dar solución a este último problema, la Dirección General para el Desarrollo de la Sociedad de la Información trabajó desde 1997 en un proyecto de receta electrónica dentro de los denominados Proyectos PISTA[321], en orden a unificar criterios a la hora de implantar la receta electrónica en las distintas CC.AA. Euskadi se incorporó a este proyecto junto a otras CC.AA como Madrid o Cataluña, comprometiéndose así a aplicar la receta electrónica en su sistema de salud[322]. Hoy día la apuesta por la receta electrónica queda reflejada expresamente en las leyes, que disponen la necesidad de tender a implantar esta herramienta[323]. Este impulso se ha traducido en la aprobación de diferentes proyectos que, como se ha visto, a nivel autonómico han ido incorporando la receta electrónica en sus sitemas de salud. La coordinación e

[315] Hoja descriptiva del Proyecto PISTA, Receta electrónica, en http://www.setsi.min.es/sat/pista/sanidad/SAN_11_C.html/.

[316] ACUÑA, "Receta Electrónica...", cit., 2002: "la receta electrónica es un medio apropiado para conocer todo el ciclo de vida de un medicamento, en sus facetas de prescripción y dispensación", lo cual evita fraudes y facilita la realización de investigaciones y estadísticas al tener mayor conocimiento de la situación en que se dan las recetas.

[317] Atendiendo a un estudio realizado en un hospital de Chicago se presume que un 60% de los errores que se cometen en un hospital al recetar medicamentos podría evitarse si el sistema de prescripción de fármacos estuviera informatizado. Diario Médico, 15 abril 2004, http://www.diariomedico.com/.

[318] HOURS, "Receta Electrónica", cit., 2002. Tanto en la Exposición de Motivos del Decreto 159/2007, 24 de julio, por el que se regula la Receta Electrónica y la Tramitación Telemática de la Prestación Farmaceútica a Cargo del Servicio Catalán de Salud, como del Decreto 206/2008, de 28 de agosto, de Receta Electrónica en Galicia y Decreto 93/2009, 24 de abril, por el que se regula la Implantación de la Receta Electrónica en el ámbito del Sistema Sanitario Público de Extremadura, se citan los principales aspectos positivos del empleo de la receta electrónica.

[319] CORDOBES, "Informática. Receta... (I)", cit., 2001: "todos estos equipos se caracterizan por la rapidez de su obsolescencia".

[320] CORDOBÉS, "Informática.Receta... (I)", cit., 2001. "Las transferencias de la sanidad y el poco interés en colaborar de las distintas comunidades autónomas hacen tener 17 sistemas sanitarios y 17 recetas electrónicas distintas, y en algunos casos no compatibles". El mismo autor, en "Informática. Receta... (II)", cit., 2002, analiza los distintos proyectos de diferentes CC.AA.

[321] http://www.setsi.min.es/sat/pista/proyectos.htm/

[322] http://www.euskadi.net/eeuskadi/

[323] Artículo 33.2 Ley, 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: "*(...) Se tenderá a la dispensación individualizada de medicamentos y a la implantación de la receta electrónica, en cuyo desarrollo participarán las organizaciones colegiales médica y farmacéutica*".

interoperabilidad entre los diferentes proyectos autónomicos se ha producido por diferentes vías. Por un lado con la aprobación de normas estatales que establecen criterios mínimos sobre las características de las recetas y su dispensación, a respetar por todos los sistemas sanitarios que componen el Sistema Nacional de Salud[324]. De esta manera las recetas serán válidas y operativas en todo el Estado. Por otro, la interoperabilidad entre los diferentes sistemas de información, que viene exigida por las normas[325], y que es necesaria para que las distintas administraciones puedan compartir datos y llevar a cabo sus funciones, se hace posible gracias a convenios como los ya citados, en los que las diferentes administraciones se comprometen a adoptar sistemas compatibles con los empleados, sobre todo, por el sistema nacional de salud.

Se puede afirmar que la receta electrónica es una aplicación que se está expandiendo y que no tardará en generalizarse. Sin embargo, las críticas que se han vertido no son pocas, centradas, sobre todo, en los riesgos que genera para el derecho a la autodeterminación informativa la transmisión de datos que requiere su uso. Es cierto que la receta electrónica trae consigo un flujo continuo de información relativa a la salud de las personas, lo cual crea riesgos evidentes[326]. Sin embargo, tal y como se ha planteado, este problema tiene un carácter eminéntemente técnico y la solución vendrá desde el ámbito científico: se trata de garantizar la seguridad en el flujo de datos, cosa técnicamente posible.

El verdadero problema generado en torno a la confidencialidad con respecto a la receta electrónica ha venido desde el ámbito del Derecho. La Ley de Medidas Fiscales, Administrativas y del Orden Social[327], en su artículo 132 introduce la receta electrónica de forma definitiva en el Sistema Nacional de Salud, pero lo hace realizando un apunte que ha generado una avalancha de críticas: "*no será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean de consecuencia de la implantación de un sistema de receta electrónica*". Esta previsión se ha recogido, también, en posteriores normas[328]. Sin duda se trata de una cuestión de gran transcendencia que más adelante se analizará con detenimiento. Ahora, basta con indicar que no parece una Ley de Acompañamiento, como es la citada, el mejor instrumento para determinar una cuestión de tal relevancia, que probablemente sería merecedora de una norma particular que regulase el tratamiento de los datos relativos a la salud.

[324] RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación.
[325] DA tercera, Decreto 181/2007, 19 de junio, por el que se regula la Receta Médica Electrónica, de la Comunidad Auónoma de Andalucía: "*El sistema informático permitirá la compatibilidad con los programas de gestión de las oficinas de farmacia y con cualesquiera otros sistemas de receta médica electrónica que se establezcan en el Sistema Nacional de Salud"*. En el mismo sentido la DA segunda del Decreto 93/2009, 24 de abril, por el que se regula la implantación de la Receta Electrónica en el Ámbito del Sistema Sanitario Público de Extremadura.
[326] ÁLVAREZ CIENFUEGOS*, "*La Aplicación...", cit., 2001.
[327] Ley 62/2003, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.
[328] Artículo 77.8 Ley 29/2006, 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios. En el mismo sentido artículo 19.2 RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación.

CAPÍTULO 2. CUESTIONES PREVIAS AL ANÁLISIS DE LOS PRINCIPIOS BÁSICOS QUE RIGEN LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SANITARIOS.

Una vez determinado el alcance de lo que se ha llamado la Sociedad de la Información y subrayada la especial importancia que la información y los instrumentos que sirven de medios de manipulación o tratamiento de la misma, las denominadas TIC, han adquirido en todos los aspectos de la vida, antes de analizar los principios fundamentales que integran el régimen jurídico de la protección de datos de carácter personal en el ámbito sanitario, se van a estudiar una serie de puntos que ayudarán a comprender mejor dichos principios.

I. LA RAZÓN DE SER DE LA LOPD EN LA SOCIEDAD DE LA INFORMACIÓN.

Corresponde en primer lugar analizar cómo se ha de interpretar, en el contexto que se ha expuesto en el capítulo anterior, el marco jurídico regulador de la protección de datos de carácter personal, teniendo presente que la forma de entender el desarrollo de las TIC condicionará la interpretación que se vaya a dar a la normativa correspondiente.

I.1. Sobre la importancia del Derecho en la Sociedad de la Información.

Se ha apuntado que el tratamiento de datos de carácter personal constituye en las sociedades actuales una operación imprescindible, que tanto sujetos privados como públicos llevan a cabo para desarrollar sus actividades[329]. Las TIC hacen posible esta manipulación y le otorgan además un alcance global. Las ventajas que las nuevas tecnologías aportan a todos los sectores de la sociedad y específicamente al sanitario ya se han señalado, por lo que no se van a repetir aquí[330]. Esta situación trae como resultado la creación de un constante flujo de informaciones por todo el planeta. Todas las posibilidades que en los diversos ámbitos de la vida ofrecen las TIC hacen que la manipulación de la información personal sea hoy una realidad innegable e inevitable[331]. La sociedad se está transformando y el eje de esta alteración lo conforma un hecho indiscutible: la mayor importancia que la información y las TIC capaces de manipularla están adquiriendo.

Uno de los principales retos de las sociedades actuales consiste en implantar y desarrollar las nuevas tecnologías en todos los ámbitos de la vida. Este reto cuenta con diferentes vertientes: tecnológica, económica, social, etc. Una de las perspectivas más relevantes a la hora de afrontar dicho desafío es la jurídica. Ante la nueva realidad el Derecho ha de jugar un papel

[329] REBOLLO DELGADO, *El Derecho...*, cit., 2000, p. 188: "El mismo riesgo de acumulación de datos, al que está sometido el individuo por la acción del Estado, surge de la acción de otros ciudadanos".
[330] TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p.12.
[331] Muestra reciente de ello es el Tratado entre el Reino de Bélgica, la República Federal Alemana, el Reino de Espala, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo, la delincuencia transfronteriza y la migración ilegal, hecho en Prüm el 27 de mayo de 2005, y ratificado por España, BOE nº 307, 25 de diciembre de 2006, en el que se abren nuevas vías para crear un flujo de información a nivel europeo, que alcanza a información derivada de análisis de ADN, con el fin, fundamentalmente, de perseguir delitos que tengan un alcance transfronterizo. GAY FUENTES, *Intimidad y tratamiento…*, cit., 1995, p. 17, subraya la necesidad de que la Administración incorpore las TIC para la realización de sus tareas.

fundamental[332], siendo necesaria la creación de un marco jurídico adecuado, dirigido a equilibrar los diferentes intereses que entran en juego al utilizar las nuevas tecnologías.

Frente a posiciones procedentes sobre todo del mundo de los cibernautas, que niegan la necesidad de normas que regulen el ciberespacio y que afirman que el tercer entorno es autorregulable[333], se interpreta aquí que los problemas que crean las TIC han de tener respuesta en el Derecho[334]. Estas nuevas herramientas están cambiando la forma de relacionarse de las personas en los diferentes campos en que desarrollan su actividad, sea pública o privada. Siendo esto así, resulta lógico apuntar que si la sociedad cambia también tendrá que hacerlo el marco normativo en el que se desenvuelven dichas relaciones[335]. La necesidad de adaptar el Derecho a esta nueva realidad, o de crear una nueva disciplina jurídica[336], es una cuestión que no es nueva pero que todavía hoy no ha sido superada o cerrada.

El Derecho nace necesariamente de la sociedad[337], "allí donde hay un ente social organizado (...) hay también Derecho"[338]. El Derecho es el instrumento a través del cual una sociedad se

[332] GAY FUENTES, *Intimidad y tratamiento…*, cit., 1995, p. 18.

[333] Como ejemplo de esta posición pueden citarse PERRY BARLOW, John *Declaración de Independencia del Ciberespacio,* Davos, 8 de febrero de 1996, y Manifiesto por el Ejercicio de una Ciberciudadanía Activa, Responsable y Activa, de 2002, etc. CARRASCOSA LÓPEZ, "La Regulación...", cit., 1998, p. 40: "La autorregulación nos lleva a "deberes informáticos de autocontrol", pactados por las empresas, los clientes y las instituciones sociales, para evitar atentados contra el honor y la libertad; para no transgredir derechos de autor; no hacer negocios con tráfico de imágenes pornográficas de niños; para impedir que se den perversamente fórmulas de confección de bombas".

[334] ÁLVAREZ RICO, "Informática y Derecho...", cit., 1998, p. 1035: señala la relevancia del Derecho, frente a la posición que fía a la autorregulación la determinación de los criterios que se han de seguir en las relaciones que se van a llevar en el ciberespacio; MARTÍNEZ MARTÍNEZ, *Una aproximación…,* cit., 2004, p. 51.

[335] FERNÁNDEZ ESTEBAN, *Nuevas tecnologías…*, cit., 1998, p. XXV.

[336] CARRASCOSA LÓPEZ, "La Regulación...", cit., 1998, p. 39; OROZCO PARDO, "Notas acerca de la relación...", cit., 1998, p. 901; PÉREZ LUÑO, *Manual de Informática...*, cit., 1996, p. 17; LÓPEZ-IBOR MAYOR y GARCÍA DELGADO, "Situación del Derecho...", cit., 1994, p. 647; VANDERBERGME, "Law and Information...", cit., 1989, p. 4. Ante los nuevos problemas que plantean las TIC las tradicionales categorías y conceptos jurídicos no sirven. El jurista tiene que enfrentarse a un fenómeno que afecta a todos los ámbitos del Derecho: penal, constitucional, administrativo, mercantil, etc..

Frente a la posibilidad de considerar que las TIC afectan a distintas disciplinas del Derecho y crear soluciones concretas para cada problema en las diferentes áreas del ordenamiento, lo cual, podría llevar a un "tratamiento fragmentario e incompleto de la problemática jurídica de la Informática", la doctrina ha optado por tender hacia la unificación de conceptos, principios, métodos, fuentes y estructuras, hasta crear una disciplina nueva, independiente, dirigida a regular el empleo de las nuevas tecnologías.

Esta nueva rama del derecho, que podría denominarse como Derecho de las Nuevas Tecnologías o de las TIC, constituiría un ordenamiento autónomo, con su propio objeto de regulación, su metodología, sus fuentes legislativas, jurisprudenciales y doctrinales.

Hay que apuntar en este momento, que cuando se está haciendo referencia a un nuevo ordenamiento, se hace entendiéndolo no como mero conjunto de normas, sino también como nuevos valores que fundamentan ese agregado normativo. La nueva realidad que las TIC han creado exige de nuevos valores que humanicen este proceso de cambio. Y estos valores tienen que guíar al Derecho en la búsqueda de un equilibrio justo de intereses en la sociedad. ALLENDE, "Informática: el...", cit., 1994, p. 83: "La utilización que se efectúe del recurso informático (...), debe necesariamente estar inspirada en la solidaridad social y en el respeto a los derechos individuales", en especial a los de intimidad y autodeterminación informativa. TÉLLEZ AGUILERA, *Nuevas Tecnologías...*, cit., 2001, p. 36: la transformación de la sociedad exigirá "incorporar al Derecho nuevos valores y criterios culturales propios de la era de la información"; ÁLVAREZ CIENFUEGOS SUAREZ, "*Confidencialidad...*", cit., 1995; MARTÍNEZ MARTÍNEZ, *Una aproximación…,* cit., 2004, p. 51.

[337] MURILLO DE LA CUEVA, "La protección...", cit., 1989, p. 602.

[338] GARCÍA de ENTERRÍA y FERNÁNDEZ, *Curso de Derecho...*, cit., 2000, pp. 67-68.

organiza[339]. En la medida en que esta sociedad se transforma, bien cambiando los anteriores parámetros en los que se desarrollaban las relaciones, o bien creando nuevos entornos en los que relacionarse como el ciberespacio, el Derecho también tiene que cambiar para que no se creen situaciones de indefensión, de inseguridad o de desequilibrio[340]. La configuración de un marco normativo bien definido es imprescindible para que los diferentes intereses que entran en juego con el avance de las nuevas tecnologías puedan encontrar un equilibrio y para que todos los agentes implicados conozcan los parámetros entre los que han de actuar.

El Derecho y todos los sujetos que de alguna manera participan en la creación e interpretación del mismo se ven obligados a reaccionar ante la llegada de las TIC[341]. La regulación de esta materia se precisa para que la entrada en la Sociedad de la Información se produzca de acuerdo a criterios de igualdad, libertad, y también de eficacia[342].

En lo que aquí interesa, el aspecto fundamental que ha de afrontar el ordenamiento es la colisión que se produce entre los diversos intereses que se persiguen con la manipulación de la información a través de las nuevas tecnologías y los derechos fundamentales. Más allá de todas sus bondades, es conocido que la transformación que aportan las TIC en la sociedad afecta a diversos derechos fundamentales. Teniendo en cuenta que las nuevas tecnologías facilitan sobremanera la manipulación de datos de carácter personal, los derechos a la intimidad y a la autodeterminación informativa pueden verse vulnerados especialmente[343]. Son muchos los ejemplos que se pueden poner atendiendo a la realidad más cercana y cotidiana. Es conocido, por ejemplo, el supuesto en que mensajes de publicidad llegan a los teléfonos móviles de los ciudadanos sin conocer la procedencia de los mismos. Este hecho es hoy día regulado por las normas, que limitan la posibilidad de enviar estas comunicaciones publicitarias sin el

[339] FROSINI, "El Jurista...", cit., 1999, p. 246: "El Derecho contempla los comportamientos de los hombres en las relaciones que éstos mantienen entre sí o con las cosas (...). La labor del jurista consiste en configurar jurídicamente dichas relaciones, esto es, de objetivarlas en normas jurídicas como hace el legislador, o bien, de controlar las conductas con las normas jurídicas, como hace el juez".

[340] GONZÁLEZ-TABLAS SASTRE, "El Derecho...", cit., 2000-2001, p. 271: "Toda transformación social impone, más tarde o más temprano, la necesidad de una regulación o si se quiere de una intervención del Derecho. Ello hará posible el disfrute de los derechos y pondrá coto a los abusos y desmanes que, inicialmente, los depabilados y más tarde los criminales cometen aprovechando la ignorancia, la buena fe y la falta de protección jurídica de sus víctimas".

[341] ; LÓPEZ-IBOR MAYOR y GARCÍA DELGADO, "Situación del Derecho...", cit., 1994, pp. 645-646; VALERO TORRIJOS, "Administración Pública...", cit., 2000, p. 2.944.

[342] CARRASCOSA LÓPEZ, "La Regulación...", cit., 1998, p. 35: "Frente a este riesgo de la informática o más concretamente de las nuevas tecnologías de la información y la comunicación, los profesionales de ésta, el público en general y especialmente los juristas pueden asumir, al menos, dos actitudes:

1.- Aceptar y someterse al Derecho tal como está regulado (...).

2.- Desarrollar una nueva legislación adecuada a los cambios que sufre la sociedad, formulando propuestas a fin de que el Derecho asuma nuevas formas que no sólo obstaculicen el uso de las nuevas tecnologías, sino que lo regulen adecuadamente, revisando y adecuando las viejas leyes a las necesidades y situaciones jurídicas que van apareciendo con las nuevas tecnologías".

[343] SAN 14 de septiembre de 2001, FJ 2. MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información…,* cit., 2001, p. 47; DRUMMOND, *Internet, privacidad…,* cit., 2004, p. 29.

consentimiento del titular[344]. Otro ejemplo actual lo pueden constituir los abusos a los derechos de las personas, que del uso de las redes sociales en Internet pueden derivar[345].

Es imprescindible, por lo tanto, crear un marco jurídico adecuado que regule la colisión entre la necesidad de manipular información y el derecho a la autodeterminación informativa. La exigencia de configurar un entorno seguro y respetuoso con los derechos fundamentales constituye una variable fundamental para que la Sociedad de la Información pueda avanzar. En este sentido, la conocida sentencia que deroga determinados apartados de la LOPD señala el importante papel que ha de jugar el legislador, ya que es el responsable de garantizar los derechos fundamentales ante el uso de la informática y demás herramientas empleadas en la manipulación de los datos[346].

La importancia de la creación de un marco jurídico adecuado se ha puesto de manifiesto en numerosas ocasiones a raíz de la aprobación de nuevas normas dirigidas a regular esta materia. En el ámbito estatal esta circunstancia se reflejó, por ejemplo, cuando se aprobó el nuevo reglamento que hoy día desarrolla la LOPD[347] y que ha sido recientemente anulado en diferentes puntos por los tribunales[348]. La AEPD subrayó la importancia de la aprobación de dicha norma como instrumento necesario para dar una mayor seguridad jurídica a los agentes implicados en los tratamientos de datos[349]. Este reglamento ha venido a llenar las lagunas jurídicas que creaba la ausencia de una norma que desarrollara específicamente la LOPD. Piénsese que, a falta de desarrollo, la Ley no lleva a cabo más que una regulación general de la protección de datos. Esta regulación genérica, cuando trata de aplicarse en la realidad, plantea numerosas dudas. La solución a estas dudas ha venido dada en gran parte con la aprobación del reglamento.

En el ámbito internacional, la importancia de crear un marco legal claro y preciso que determine los parámetros en los que se han de manipular los datos de carácter personal se ha subrayado sobre todo a partir del 11-S, momento en el que la necesidad de crear un flujo de

[344] Artículo 21 Ley 34/2002, 11 de julio, de Servicios de la Sociedad de la Información y el Comercio Electrónico. Resolución de la AEPD R/00535/2008, 9 de mayo de 2008. Procedimiento PS/00431/2007.

[345] Resolución sobre protección de la privacidad en los servicios de redes sociales, adoptada en la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad, 15-17 de octubre de 2008. Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 5/2009, sobre las redes sociales en línea, 12 de junio de 2009.

[346] STC 30 de noviembre del 2000, FJ 4, que viene a dar continuación a las consideraciones teóricas que planteaba a este respecto la STC 20 de julio de 1993, FJ 6, que ya apuntaba los primeros pasos en la configuración del derecho fundamental a la autodeterminación informativa, partiendo de la consideración de la informática como una amenaza.

[347] PIÑAR MAÑAS, "El Porqué de un Reglamento…", cit., 2007, pp. 9-34, analiza la razón de ser del RDLOPD.

[348] STS 15 de julio de 2010, que anula, por disconformes a derecho, los artículos 11, 18, 38. 2, y 123.2 de la disposición reglamentaria, así como la frase del artículo 38.1 .a) que dice así: "... y al respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero".

[349] Memoria de la AEPD, 2003, en la que la Agencia llama la atención sobre la necesidad de una norma que entre a desarrollar la LOPD; Memoria de la AEPD, 2007, en la que se subraya la importancia del nuevo reglamento para aclarar y concretar diferentes aspectos de la LOPD. El Dictamen del Consejo de Estado, nº 1909/2007, 15 de noviembre de 2007, sobre el Proyecto Real Decreto por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se refiere también a la necesidad de aprobar dicho reglamento como instrumento normativo que ha de dar una gran seguridad jurídica, al aclarar diferentes aspectos de la LOPD. PIÑAR MAÑAS, "El Porqué de un Reglamento…", cit., 2007, pp. 30-31; PUENTE ESCOBAR, "Ámbito objetivo…", cit., 2008, p. 27.

información de alcance internacional adquiere una nueva dimensión[350]. Ante la necesidad de configurar dicho flujo de información con el fin fundamental de luchar contra el terrorismo y garantizar la seguridad, resulta obligatoria la creación de un marco normativo que garantice la protección de los derechos fundamentales de la ciudadanía en todo momento. Un supuesto concreto en el que han entrado en colisión en el ámbito internacional la necesidad de manipular información y la obligación de salvaguardar el derecho a la autodeterminación informativa, lo constituye la obligación impuesta a los proveedores de servicios de comunicaciones accesibles al público de conservar durante un periodo de tiempo los datos relativos a las comunicaciones de la ciudadanía[351]. Evidentemente, dicha obligación afecta al derecho a la autodeterminación informativa de los titulares de los datos que se conservan. Las normas europeas han tratado de encontrar el equilibrio entre dicha obligación y la necesidad de proteger el indicado derecho.

[350] Documento del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, "The Future of Privacy", 1 de diciembre de 2009.

[351] En el ámbito europeo la solución la daba la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, 12 de julio de 2002, relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas, que en su artículo 15.1 señalaba que "*Los Estados miembros podrán adoptar medidas legales para limitar el alcance de los derechos y las obligaciones que se establecen en los artículos 5 y 6, en los apartados 1 a 4 del artículo 8 y en el artículo 9 de la presente Directiva, cuando tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE. Para ello, los Estados miembros podrán adoptar, entre otras, medidas legislativas en virtud de las cuales los datos se conserven durante un plazo limitado justificado por los motivos establecidos en el presente apartado. Todas las medidas contempladas en el presente apartado deberán ser conformes con los principios generales del Derecho comunitario, incluidos los mencionados en los apartados 1 y 2 del artículo 6 del Tratado de la Unión Europea*". La aprobación posterior de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la Conservación de Datos Generados o Tratados en Relación con la Prestación de Servicios de Comunicaciones Electrónicas de Acceso Público de Redes Públicas de Comunicaciones y por la que se modifica la Directiva 2002/58/CE, da una nueva dimensión a este conflicto de intereses al señalar en su artículo 3 que 1. "*Como excepción a los artículos 5, 6 y 9 de la Directiva 2002/58/CE, los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.*
2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas en las que los datos los generan o tratan, y conservan (en lo que a los datos telefónicos se refiere) o registran (en lo que a los datos de Internet se refiere), proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo la jurisdicción del Estado miembro de que se trate en el marco de la prestación de los servicios de comunicaciones en cuestión. La conservación de datos en relación con las llamadas no conectadas no será obligatoria con arreglo a la presente Directiva". Esta Directiva ha sido desarrollada en el ámbito interno por la Ley 25/2007, de 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicación. Recientemente, la STC Alemán 2 de marzo de 2010 ha declarado nulas determinadas disposiciones de la Ley que desarrolla la Directiva que se acaba de citar, en la medida en que considera que no cumple con el principio de proporcionalidad, vulnerando el derecho a la protección de datos. Esta decisión saca a la palestra la conveniencia de reinterpretar leyes como la española, que obligan a los operadores a conservar determinados datos de los usuarios de los medios de telecomunicación. Al poner en tela de juicio el contenido de la normativa alemana se pueden llegar a cuestionar normativas semejantes como la española. Como ya dijera la doctrina, es necesario atender al principio de proporcionalidad a la hora de interpretar el contenido de dichas leyes, para que las autoridades, fundamentalmente las Fuerzas y Cuerpos de Seguridad, no cuenten con un espacio excesivamente amplio a la hora de manipular los datos de carácter personal que los operadores están obligados a conservar. CUBERO MARCOS y ABERASTURI GORRIÑO, "Protección de los Datos…", cit., 2008, pp. 191-192.

Con estas premisas, la realidad es que en relación a la concreta colisión entre la necesidad de manipular información de carácter personal en las sociedades actuales y la obligación de proteger el derecho fundamental a la autodeterminación informativa, el Derecho no ha dado una respuesta del todo satisfactoria, ni en el ámbito internacional ni en el estatal. Hoy día, en lo que aquí interesa, la base de este marco jurídico la componen la Directiva europea relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y la LOPD. En los próximos apartados se irán desgranando los aspectos más relevantes de estas normas. Sin embargo, se puede evidenciar desde ahora que en lo que toca al sector de la salud las normas van, otra vez, por detrás de la realidad[352], y la necesidad de crear un marco jurídico adecuado no se ha visto satisfecha del todo, fundamentalmente por dos motivos.

Primero, porque la base que componen ambas normas necesita ser desarrollada para que no existan lagunas jurídicas. En el ámbito sanitario este desarrollo presenta todavía grandes deficiencias. El marco jurídico, que en el ámbito interno regula la protección de datos sanitaria, deja mucho que desear, fundamentalmente porque son numerosos los aspectos que todavía hoy siguen sin tener respuesta. Segundo, porque el marco jurídico no ha sabido adaptarse a las exigencias que plantea el carácter global o internacional de los problemas que nacen de la aplicación de dichos instrumentos. Las autopistas de la información tienen un alcance global y frente a esta situación el Derecho no ha sido todavía capaz de dar una respuesta de la misma dimensión[353]. Ejemplo de lo dicho es el hecho de que ante la ciberdelincuencia, que también afecta al ámbito sanitario y que tiene alcance internacional, la normativa penal de los diferentes estados dista mucho de estar unificada[354].

La ya derogada LORTAD admitía que "*el inevitable desfase que las normas de Derecho positivo ofrecen respecto de las transformaciones sociales es, si cabe, más acusado en este terreno, cuya evolución tecnológica es especialmente dinámica*"[355]. Es cierto que la sociedad está avanzando a una gran velocidad y que, como afirma la doctrina, la tardía reacción del Derecho es justificable, de alguna manera, "por la prudencia que debe impregnar su evolución dadas las consecuencias tan relevantes que las normas jurídicas implican"[356]. Sin embargo, esta justificación no puede llevar, como parecía hacer la LORTAD, a asumir desde un inicio, que ante los nuevos escenarios que plantea el imparable avance de las TIC el Derecho no puede reaccionar de forma adecuada.

[352] HERRÁN ORTIZ, *La Violación...*, cit., 1998, p. 121.
[353] PÉREZ LUÑO, "Derecho y nuevas tecnologías…", cit., 2005, p. 232; MUÑOZ MACHADO, *La regulación de la red…*, cit., 2000, p. 49; GUERRERO PICÓ, *El Impacto de Internet…*, cit., 2006, p. 331-339, pone de manifiesto los problemas que causa la desregulación de la Red de Redes; PALOMAR OLMEDA y PÉREZ GONZÁLEZ, "La Protección de Datos…", cit., 2008, p. 45; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 244.
[354] SÁNCHEZ BRAVO, "Una Política...*",* cit., 2001; SÁNCHEZ BRAVO, "El Convenio...*",* cit., 2002; GÓMEZ NAVAJAS, *La Protección…*, cit., 2005, p. 47.
[355] Exposición de Motivos LORTAD.
[356] VALERO TORRIJOS, "Administración Pública...", cit., 2000, p. 2944.

I.2. Sobre la necesidad de adoptar una posición flexible a la hora de crear e interpretar el marco jurídico dirigido a regular la protección de datos.

Como se acaba de ver, ante los retos que plantea la Sociedad de la Información el Derecho ha de jugar un papel fundamental a la hora de encontrar un equilibrio entre los diferentes intereses en juego[357]. Este equilibrio hay que buscarlo principalmente cuando un bien jurídico se erige en argumento para limitar otro. En el momento en que se produce una confrontación entre derechos, principios, valores, intereses u otros bienes jurídicos, unos se constituyen en límites de los otros. En lo que aquí interesa, el derecho a la autodeterminación informativa puede verse limitado por una manipulación de datos que persigue una finalidad concreta. Por ejemplo, y atendiendo a decisiones que los tribunales han adoptado tanto en el ámbito interno[358] como en instancias internacionales[359], se ha visto cómo en el sector laboral se ha pretendido emplear las nuevas tecnologías como sistema de control de los trabajadores, o en el policial se han tratado de utilizar nuevas herramientas como métodos de identificación de personas. La finalidad de controlar a los trabajadores o de investigar determinados delitos constituye la base para limitar el derecho a la autodeterminación informativa. En este tipo de situaciones el Derecho ha de aportar los criterios suficientes para que las colisiones entre diferentes bienes jurídicos se resuelvan de forma que se encuentre un equilibrio entre los distintos intereses afectados.

Se trae aquí esta reflexión porque ante los nuevos problemas que genera la Sociedad de la Información el Derecho puede actuar de formas diferentes. A la hora de encontrar el equilibrio entre la necesidad actual de manipular información de carácter personal y de emplear las nuevas tecnologías, y la obligación de salvaguardar el derecho a la autodeterminación informativa, el Derecho podría adoptar tres posiciones. La primera consistiría en una postura garantista con respecto al derecho a la autodeterminación informativa. Desde esta posición las nuevas tecnologías podrían verse como "enemigas" de los derechos fundamentales. La informática y la aparición de Internet constituirían una amenaza para dichos derechos. Esta perspectiva conllevaría como consecuencia principal la adopción de criterios restrictivos con respecto al uso

[357] Preámbulo Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, venía a recoger esa idea al considerar que "*(...) en un escenario que tiende a una socialización creciente de la información mediante la tecnología, hay que tener una clara conciencia de los riesgos que implica un mal uso de esta información y los eventuales efectos no deseados en las libertades y los derechos fundamentales de la persona. De ahí proviene la necesidad de desarrollar un marco legal adecuado para afrontar la problemática que, para el ejercicio efectivo de estos derechos, plantea el nuevo contexto social"* (Esta Ley ha sido derogada por la Ley 32/2010, de 1 de octubre de 2010, de la Autoridad Catalana de Protección de Datos).. En este mismo sentido Exposición de Motivos Ley 2/2004, de 25 de febrero, de ficheros de datos de carácter personal de titularidad pública y de creación de la Agencia Vasca de Protección de Datos considera que los "*(...) ordenamientos jurídicos no pueden permanecer insensibles ante la eventualidad de usos perversos de las posibilidades tecnológicas, en detrimento de espacios que deben quedar reservados a la intimidad". Esta tensión entre tecnología, especialmente en el campo de la informática, e intimidad de las personas apela a una actuación legislativa que procura un equilibrio satisfactorio entre dos bienes dignos de protección jurídica".*

[358] SSTSJ de Cantabria 18 de enero de 2007, FJ 3, apunta que "el hecho de que no se halle vedada la utilización de las nuevas tecnologías entre los instrumentos disponibles para el control y vigilancia de la actividad laboral, no comporta que su aplicación pueda hacerse de manera omnímoda e indiscriminada, con abstracción de los derechos fundamentales del trabajador"; 28 de marzo de 2003, FFJJ 9 y 10, en los que se plantean las bondades y efectos negativos de un nuevo sistema de control de acceso de trabajadores a su lugar de trabajo, a través de un sistema de infrarrojos que reconoce determinada información biométrica.

[359] STEDH 4 de diciembre de 2008, S y Marper v. Reino Unido, FJ 112: "El Tribunal considera que todo Estado que reivindique el rol de pionero en la evolución de nuevas tecnologías tiene la responsabilidad particular de hallar el equilibrio justo en la materia".

de las TIC. La segunda posición, en vez de partir de esa consideración negativa de las nuevas tecnologías, pasaría a comprender esos instrumentos como mecanismos de desarrollo de los diferentes aspectos de la realidad. Esto no quiere decir que se banalice la relevancia del derecho a la autodeterminación informativa, sino que simplemente se pone el acento en la necesidad de establecer un equilibrio entre ambos factores, sin que se parta de una perspectiva negativa de las TIC que pudiera llegar a condicionar o limitar en exceso su uso. Por último, se podría encontrar una tercera posición, contraria a la primera, que decantase la balanza a favor del uso de las nuevas tecnologías en cualquier circunstancia, lo cual podría conllevar a que los derechos a la intimidad y la autodeterminación informativa quedasen vacíos de contenido.

La importancia de adoptar una u otra de las posiciones que se han señalado se puede ver reflejada sobre todo a la hora de interpretar los límites o las excepciones al derecho fundamental a la autodeterminación informativa. En caso de que se apueste por una postura garantista del citado derecho, los límites al mismo se entenderán de forma especialmente restrictiva. En caso contrario, estos límites pueden interpretarse de manera más laxa o amplia.

Las diferentes posiciones a la hora de interpretar la tensión entre la necesidad de manipular información de carácter personal y la obligación de proteger en todo caso el derecho a la autodeterminación informativa se pusieron de manifiesto en sede parlamentaria, cuando se discutieron los proyectos de la LORTAD y la LOPD. En ambos casos se podía identificar la preocupación del legislador de proteger los derechos de intimidad y de autodeterminación informativa ante el uso abusivo de las nuevas tecnologías[360]. En relación a la Ley actual, el principal punto de crítica por parte de algunos grupos parlamentarios lo constituía la ambigüedad de muchos de los términos de la Ley, que abren la puerta a la posibilidad de realizar interpretaciones excesivamente amplias de las excepciones al derecho a la autodeterminación informativa[361]. Frente a esta posición, otras posturas criticaban una visión ingenua, excesivamente garantista, del derecho a la autodeterminación informativa, afirmando que la realidad exige la manipulación de los datos, siendo necesario en muchos casos limitar el derecho a la autodeterminación informativa de las personas. Ambas visiones dan fe de las diferentes posturas que se pueden adoptar a la hora de interpretar los preceptos de una Ley.

Si se atiende a la hoy derogada LORTAD y a la vigente LOPD se observará que puede encontrarse base suficiente para apoyar, en la primera, una visión garantista o, en la segunda, una postura más relajada con respecto a la posibilidad de manipular información. Si bien en la práctica, y en cuanto a su contenido, ambas guardan gran similitud, lo cierto es que las dos normas parecen partir de una consideración diferente de cómo han de entenderse las nuevas

[360] Diario de Sesiones del Congreso de los Diputados, nº 151, 28 de noviembre de 1991: "Esta tensión entre el flujo de la información y la garantía de los derechos explica también la dificultad de una regulación en el plano internacional que empieza a adquirir cuerpo, especialmente a partir del año 1981".

[361] Diario de Sesiones del Congreso de los Diputados, nº 744, 15 de septiembre de 1999: "Cuando hemos visto en el texto de este proyecto de ley los capítulos que hablan de excepciones y restricciones, se nos han encendido luces de cautela por entender que se está entrando en una zona de carencia de sensibilidad cuando el proyecto debería (…) dirigirse a las garantías de la persona, y diría incluso, con este proyecto de ley y ante la agresividad de la técnica informática, a las garantías reforzadas. Si no somos capaces de introducir garantías reforzadas en esta sensibilidad y protección de los datos de carácter personal el proyecto puede terminar, como el anterior ante el Tribunal Constitucional".

tecnologías. La derogada Ley de 1992, haciendo suya la redacción del artículo 18.4 CE, parecía tomar como base una perspectiva negativa de las TIC. Apuntaba como objetivo limitar el empleo de la informática y otras herramientas o medios de tratamiento de datos[362]. No parece que pueda haber duda de que esta redacción dejaba entrever la idea de que la informática es un elemento peligroso[363]. La vigente Ley, por el contrario, hace hincapié no ya en la necesidad de "limitar" las nuevas tecnologías, lo cual podría conducir a posiciones excesivamente garantistas, sino en la necesidad de "potenciar" los derechos fundamentales frente al uso de las TIC[364]. Así lo hacen también la Directiva europea[365] y el Convenio del Consejo de Europa de 1981[366].

Hoy día supone un lugar común afirmar que la LOPD ha constituido un avance con respecto a la derogada LORTAD en el entendimiento del conflicto entre la informática y el respeto a los derechos fundamentales[367]. Se está de acuerdo con la corriente doctrinal que subraya la importancia de interpretar la LOPD partiendo de una idea positiva de las TIC, como medios para mejorar la sociedad[368]. El fin último de la Ley no tiene que ser el de limitar estas herramientas, sino "asegurar un uso democrático de la *information technology"*[369].

Partiendo de lo dicho en las líneas precedentes se entiende que es importante aclarar desde ahora la posición que se va a adoptar en este trabajo en relación a la consideración que merecen las TIC y la manipulación de la información como realidades que entran en conflicto con el derecho a la autodeterminación informativa. Sin ánimo de realizar un estudio filosófico sobre esta cuestión, simplemente se pretende adelantar una idea que se tendrá en cuenta al interpretar las colisiones que se producen entre diversos intereses cuando se manipulan datos de carácter personal en el ámbito sanitario. La posición que se adopte condicionará la forma de interpretar los preceptos que completan la LOPD. Una postura excesivamente beligerante en la interpretación

[362] Artículo 1 LORTAD: "*La presente Ley Orgánica tiene por objeto limitar el uso de la informática y otras técnicas"*, lo que exponía esa visión negativa de las TIC de la que partía la norma, al entender las mismas como un peligro para los Derechos Fundamentales. Si bien es verdad, como dice MURILLO DE LA CUEVA, *Informática y Protección...,* cit., 1993, p. 39, que "limitarla no es prohibirla", se está de acuerdo con TÉLLEZ AGUILERA, *La Protección...*, cit., 2002, p. 236, cuando afirma que la LORTAD parte de una "filosofía proteccionista (...) negativa"; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 77, reconoce que la redacción del artículo 18.4 CE manifiesta una postura de recelo frente a la informática.

[363] PÉREZ LUÑO, *Derechos Humanos...*, cit., 1991, p. 364, considera que la "propia fórmula <<La Ley limitará el uso de la informática...>> con que se inicia el apartado 4 del artículo 18 no es, en modo alguno casual, sino que evidencia la postura defensiva adoptada en el debate constitucional. Con ello, se puso el énfasis en la dimensión negativa de la libertad informática".

[364] Artículo 1 LOPD: "*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*". APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 23; OROZCO PARDO, "La Protección...", cit., 2002, p. 185.

[365] Artículo 1 Directiva 95/46/CE: "*Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales*".

[366] Artículo 1 Convenio 108/1981 del Consejo de Europa: "*El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de datos de carácter personal correspondientes a dicha persona*".

[367] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 25; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 51; MURILLO DE LA CUEVA, "Objeto de la Ley…", cit., 2010, p. 76.

[368] REBOLLO DELGADO, *Derechos Fundamentales...*, cit., 2004, p. 143.

[369] PÉREZ LUÑO, "La Protección...", cit., 1979, p. 68.

del papel que las nuevas tecnologías han de jugar en la sociedad actual podría llevar a cerrar el camino a instrumentos y alternativas manifiestamente positivas para sectores como el sanitario. Como se verá más adelante, podría conducir a interpretar los preceptos de la LOPD de tal manera que fuera imposible realizar, cualquiera que fuera la circunstancia, una transferencia internacional de datos de salud con fines de investigación a un país que no guarda un nivel de protección adecuado, sin necesidad de recabar la autorización del Director de la AEPD. Por el contrario, una posición excesivamente laxa y abierta conllevaría la posibilidad de aplicar las excepciones al derecho a la autodeterminación informativa de manera tan amplia que vaciaría de contenido el citado derecho.

Se entiende aquí que tratar de limitar la aplicación y desarrollo de las TIC en el tratamiento de la información, tomando como fundamento una visión eminentemente negativa del uso de las mismas, constituye una perspectiva errónea de lo que es el empleo de las nuevas tecnologías[370]. No se pueden interpretar estos instrumentos y las posibilidades de manipulación de datos que con ellas se consiguen como una amenaza, sino como una posibilidad de mejorar diversos aspectos de la vida[371]. Sin embargo, asumida esta posición, tampoco se puede negar la evidencia: las TIC mal empleadas son un riesgo para los derechos fundamentales de las personas, en particular para el de la autodeterminación informativa.

Como bien señala la Directiva europea reguladora de la protección de datos de carácter personal, las nuevas tecnologías constituyen herramientas que están al servicio de las personas[372]. Es decir, si bien cabe partir de una valoración positiva de las TIC, este punto de vista tampoco puede llevar a la consideración de que la manipulación de la información de carácter personal puede desarrollarse en todo caso, sin límite alguno. Y se subraya esta idea porque en algunos casos, si bien no se ha llegado a ese extremo, de diferentes textos de carácter internacional parece desprenderse una posición especialmente laxa ante el empleo de las nuevas tecnologías y la manipulación de datos de carácter personal. La necesidad de que la protección de la intimidad y el derecho a la autodeterminación informativa no constituyan un obstáculo para el tratamiento y, como más adelante se verá, para el flujo de la información, se subraya en distintos documentos. Desde la OCDE se ha expresado en alguna ocasión claramente esta idea haciendo referencia a la necesidad de crear un movimiento internacional de datos que favorezca el desarrollo de la ciencia médica[373].

[370] TONIATI, "Libertad Informática...", cit., 1991, pp. 140-141, concluye que "si el imperativo postulado por la sociedad de la información es el de la libre circulación de los datos, el fundamento de una sociedad de la información *democrática* no puede sino estar tendencialmente inspirado en un criterio de reciprocidad entre el Estado-aparato y los ciudadanos". Es por ello por lo que según el autor "sería ilusoria la (falsa) alternativa de intentar atenuar la demanda de información, que es, hoy por hoy, vital para el buen funcionamiento del sistema. Mucho más realista y funcional resulta actuar (...) reglamentando y racionalizando los flujos informativos"

[371] REBOLLO DELGADO, *Derechos Fundamentales…*, cit., 2004, p. 55; GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, pp. 43-44.

[372] Considerando 2 Directiva 95/46/CE.

[373] Documento de Trabajo de la OCDE, *Data Protection in Transborder Flows of Health Research,* 10 de diciembre de 1999. En el mismo sentido Recomendación del Consejo de la OCDE sobre "Directrices que regulan la protección de la privacidad y el flujo transfronterizo de datos personales", 23 de septiembre de 1980: este organismo recomienda: "que los países miembros se esfuercen por eliminar o evitar que aparezcan, en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales".

Desde finales de los 60 se han ido sucediendo las normas de carácter general tendentes a regular la protección de las personas en lo que se refiere a sus datos[374]. Hoy día parece que se está culminando un proceso en el que en el ámbito internacional los países tratan de ponerse de acuerdo en la asunción de una serie de principios, que van a constituir el núcleo del derecho a la autodeterminación informativa[375]. En el Estado español la asunción de estos criterios se produce con la aprobación de la LOPD. Su articulado compone la base reguladora de una materia especialmente complicada tanto por su carácter técnico como por la cantidad de realidades que quedan afectadas por dicha norma. La interpretación de estos preceptos, y de los demás que de alguna forma entran a regular esta materia, debiera hacerse atendiendo a lo que se ha dicho en las líneas que anteceden. Como se ha visto, la Ley actual, en contraposición a la LORTAD, no parte de una perspectiva negativa de la informática, entendida como una realidad que hay que limitar, sino que parece tomar como base una valoración más positiva de las TIC. Esta perspectiva, sin embargo, no puede llevar a adoptar una postura definitivamente contraria a la garantista a la hora de interpretar todas las disposiciones de la Ley. Hay que volver a subrayar, que cada precepto deberá interpretarse de acuerdo a las circunstancias que presente el caso al que se aplique. Esta previsión que podría resultar evidente, ha de ser puesta de manifiesto desde ahora para entender que ideas preconcebidas sobre la necesidad de realizar siempre la interpretación más favorable al derecho a la autodeterminación informativa o la contraria, deberán ser evitadas a favor de una visión más práctica que trate de analizar los enfrentamientos entre los intereses en juego atendiendo a las características particulares de cada caso.

II. LA DETERMINACIÓN DEL MARCO NORMATIVO REGULADOR DE LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL SANITARIOS.

II.1. Sobre la necesidad de una norma concreta que regule el tratamiento de datos de carácter personal en el ámbito sanitario.

El planteamiento que se acaba de hacer en el apartado anterior ha de tener aplicación en el ámbito concreto de la salud. Es conocido, y así se ha puesto de manifiesto en innumerables ocasiones[376], que en el sector de la sanidad son muchos los intereses en juego. En primer lugar, los del ciudadano, a que se le preste una asistencia sanitaria de calidad y a que en dicha prestación se respeten sus derechos fundamentales. En segundo, los del centro, a que se gestionen con la mayor eficacia posible los recursos. Y por último, los de la sociedad, a que se realicen investigaciones para el adelanto de la ciencia y para la salvaguarda de la salud pública, a que se controle el gasto, y en general al buen funcionamiento de la sanidad.

---

[374] PÉREZ LUÑO, *Derechos Humanos...,* cit., 1991, p. 351. Es en 1969 cuando nace la propuesta de ley británica sobre el control del proceso de datos denominada *data surveillance bill,* considerada como "el primer proyecto normativo en la materia" de protección de datos de carácter personal, Puede leerse un estudio sobre el origen y evolución de las normas sobre protección de datos en LOSANO, PÉREZ LUÑO y GUERRERO MATEUS, *Libertad Informática...*, cit,. 1989.

[375] *Propuesta conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal,* acogida por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 5 de noviembre de 2009.

[376] Párrafo 1.3.5 *Opinión of the European Group on Ethics in Science and New Technologies to the European Commission* de 30 de Julio de 1999.

Estos intereses pueden entrar en colisión en diferentes circunstancias. Uno de los principales conflictos que se genera en este campo es el que se produce entre la necesidad de manipular información de carácter personal y la obligación de proteger en todo caso los derechos a la intimidad y a la autodeterminación informativa de las personas[377]. En este sector la indicada dialéctica constituye uno de los grande debates[378]. Es claro exponente de lo dicho el alto número de consultas que se realizan en las diferentes agencias de protección de datos en torno a esta materia[379].

Se ha apuntado ya la importancia que una información veraz y correctamente organizada reviste en el ámbito sanitario[380]. También se ha señalado la relevancia de que la salvaguarda de los derechos fundamentales constituya una máxima a respetar cuando se manipule dicha información[381]. La necesidad de cohonestar ambos intereses se refleja en las normas dedicadas a la regulación de la actividad sanitaria y de la protección de datos de carácter personal[382].

La función del Derecho no puede ser otra que la de buscar el equilibrio entre estos diferentes bienes jurídicos en juego[383], de tal forma que todos los agentes implicados encuentren sus intereses protegidos, aunque sea dentro de unos mínimos[384]. Si bien es cierto que la solución no

[377] FROSINI, "Problemas Jurídicos...", cit., 1987, p. 50: habla del "contraste entre el <<poder informático>>de quien dispone de los bancos de datos personales en los que están fichados los individuos, y la <<libertad informática>> de poder disponer de los propios datos personales referidos a la vida privada".

[378] TRONCOSO REIGADA, "*La protección de datos*...", cit., 2008, pp. 13-14.

[379] El 25% de las consultas realizadas a la Agencia de Protección de Datos de la Comunidad de Madrid se refieren al ámbito sanitario, como declaró MARÍN PÉREZ, Subdirector General de inspección y tutela de derechos de la agencia en la revista *Diariomedico.com* de 1 de octubre de 2004, en http://www.diariomedico.com/. Del mismo modo, la Memoria de 2003 de la Agencia Española de Protección de Datos subraya que de entre todos los datos calificados como especialmente protegidos, "son los de salud los que están suscitando en la realidad mayores problemas".

[380] Relevancia que se plasma en la Circular nº 9/97, de 9 de julio del INSALUD que recoge las instrucciones generales sobre seguridad y protección de datos y que señala que los *"sistemas informáticos del INSALUD constituyen un elemento básico de gestión en el sistema sanitario que debe ser objeto de una especial protección"*.

[381] GIMENO SENDRA, "Información Clínica…", cit., 1997, p. 222.; HERRÁN ORTIZ, *La violación...*, cit., 1998, p. 177.

[382] Es claro exponente de ello el que en recientes normas dedicadas a regular esta cuestión se haga referencia expresa a la necesidad de proteger el derecho a la autodeterminación informativa de los pacientes: Artículo 3.6 RD 223/2004, 6 de febrero de 2004, por el que se regulan los Ensayos Clínicos con Medicamentos: "*El tratamiento, comunicación y cesión de los datos de carácter personal de los sujetos participantes en el ensayo se ajustará a lo dispuesto en al ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y constará expresamente en el consentimiento informado*". Artículo 6 RD 831/2010, 25 de junio de 2010, de Garantía de la Calidad Asistencial de la Prestación a la Interrupción Voluntaria del Embarazo: "*1. Los centros o establecimientos públicos o privados acreditados conservarán la historia clínica y los dictámenes, informes y documentos que hayan sido precisos para la práctica de la interrupción voluntaria del embarazo, así como el consentimiento expreso de la mujer embarazada. 2. Los centros que presten la interrupción voluntaria del embarazo garantizarán la intimidad de las mujeres y la confidencialidad del tratamiento de sus datos de carácter personal, conforme a lo previsto en la Ley Orgánica 2/2010, de 3 de marzo*".

[383] RUIZ MARTÍNEZ, "España: el Derecho...", cit., 2002, en http://www.premium.vlex.com/; MÉJICA GARCÍA, *El Enfermo Transparente*..., cit., 2004, pp. 25-26:expone los problemas con los que el Derecho se puede enfrentar con la creación de la historia clínica.

[384] Es necesario apuntar que en un ámbito como el sanitario en el que el componente humano está tan presente, la solución a los conflictos no vendrá exclusivamente por la vía del derecho, sino también con la concienciación de los profesionales de que el paternalismo con el que anteriormente afrontaban la relación médico-paciente ha quedado ya obsoleto, con la asunción de la idea de que el paciente es mayor de edad y capaz de tomar sus propias decisiones. Como señala el Grupo de Expertos en Información y Documentación Clínica en su Documento final de 26 de noviembre de 1997, "el aprendizaje de esta nueva relación exige cambios de mentalidad en los profesionales que no se consiguen sólo

sólo se encontrará en las normas, pues como en todos los sectores, también en el sanitario la norma deberá estar acompañada por medidas tendentes a concienciar a los profesionales y pacientes, no ya del tantas veces citado cambio producido en la forma de entender la relación médico-paciente ahora fundamentada en el principio de autonomía del paciente, sino de la importancia de salvaguardar el derecho a la protección de datos de los pacientes[385], no es menos cierto que la configuración de un marco legal adecuado resulta indispensable para que la búsqueda del equilibrio entre los intereses citados se resuelva de manera satisfactoria.

Las referencias en las normas a este conflicto de intereses son varias y se encuentran en textos legales dirigidos a regular la materia sanitaria y la protección de los datos de carácter personal. En el primer caso, las normas muestran plena sensibilidad en relación a esta problemática, planteando como reto de primer orden el respeto a la intimidad y a la autodeterminación informativa de los ciudadanos[386]. En cierta medida no es de extrañar que así sea, si se tiene en cuenta que la intensidad del debate en torno a los peligros que resultan del empleo de las nuevas tecnologías en el ámbito sanitario es hoy día mayor que en momentos anteriores[387]. En el segundo caso también puede afirmarse que es así, si se atiende a las referencias que la normativa reguladora de la protección de datos realiza a los datos de salud.

"a golpe de decreto", sino mediante la implantación de medidas educativas, formativas y de participación de los profesionales".

[385] En la práctica cotidiana de los hospitales, son muchas las actitudes de los profesionales que pueden suponer una agresión a esta libertad y al derecho a la intimidad de las personas. La desaparición de hechos tan comunes como la exposición en tablones de documentos con informaciones de los pacientes, o los comentarios desmedidos en los pasillos entre profesionales de un centro, constituye un objetivo a cumplir. CASARES, "Es muy difícil…", cit., 2004.

[386] Artículo 10 LGS: "*Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias: 3. A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público*; Artículo 2.1) LBAP, que establece que *"La dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica";* Artículo 5.1.c) Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias, que determina como principio general informador de la relación entre profesional sanitario y paciente *"El deber de respetar la personalidad, dignidad e intimidad de las personas a su cuidado";* Artículo 19 Ley 55/2003, de 16 de diciembre, del Estatuto Marco del Personal Estatutario de los Servicios de Salud, que en su apartado i) obliga a "*respetar la dignidad e intimidad personal de los usuarios",* y en su apartado j), determina el deber de mantener *"la debida reserva y confidencialidad de la información y documentación relativa a los centros sanitarios y a los usuarios obtenida, o a la que tenga acceso, en el ejercicio de sus funciones"*. Artículo 1.e) Decreto 175/1989 de 18 de julio, por el que se aprueba la Carta de Derechos y Obligaciones de los Pacientes y Usuarios del Servicio Vasco de Salud/Osakidetza. Y al igual que las normas, los principales códigos deontológico también han mostrado una especial sensibilidad con el respeto a la intimidad. Así el Código Internacional de Ética Médica de 1949 enmendada en 1968 y 1983 que entiende que *"el médico debe guardar secreto de todo lo que se le haya confiado",* y, como no, el artículo 17.1 del Código de Ética y Deontología médica de 1999 que dispone que los *"sistemas de informatización médica no comprometerán el derecho del paciente a su intimidad"*.

[387] Es innegable que a día de hoy los ciudadanos muestran una mayor preocupación por el empleo que se da a sus datos, no hay más que ver el aumento constante del número de denuncias realizadas ante las diferentes Agencias de Protección de Datos. Sin embargo, esta afirmación podría chocar con la realidad que se vive en las televisiones donde la gente se dedica constantemente a desnudar su interior en público. Ciertamente, si bien en la mayoría de las normas que en mayor o menor medida tocan el problema de la protección de datos, se hace referencia a una preocupación social por la salvaguarda de los derechos a la intimidad y a la autodeterminación informativa, como lo hace la Ley 12/1989 de 9 de mayo de la Función Estadística Pública que en su exposición de motivos habla de *"la creciente preocupación de los ciudadanos por el manejo informático de datos que les conciernen"*, lo cierto es que hay datos que muestran que el interés real de tales ciudadanos por la protección de sus datos no es tan grande como en un principio debía serlo. Es especialmente significativo el caso de los trabajadores de una empresa londinense que revelaron la contraseña de su

Sin embargo, y a pesar de esta inicial muestra de sensibilidad respecto a la materia que aquí se estudia, el vigente marco legal plantea problemas de envergadura. El principal es que las referencias concretas a la problemática que en este trabajo se analiza no son especialmente amplias y no se prodigan en la regulación de esta cuestión. La LOPD, junto a las correspondientes leyes autonómicas, regula la protección de datos de carácter personal en todos los ámbitos y situaciones en que estos datos puedan ser manipulados. Esta norma tiene, por lo tanto, carácter general. En el ámbito interno no existen normas dirigidas a regular estas cuestiones, al contrario de lo que ocurre, por ejemplo, en el ámbito del Consejo de Europa, donde han sido aprobadas normas concretas para regular los problemas específicos que se crean en la manipulación de datos en sectores determinados como el sanitario[388].

En la regulación realizada por la LOPD las referencias más claras a los datos de salud se encuentran en los artículos 7[389] y 8[390]. La coexistencia de estos dos preceptos ha generado problemas de interpretación que serán resueltos más adelante. Interesa ahora acercarse a la letra de la segunda disposición para determinar cuál es el marco legal en el que ha de resolverse el conflicto jurídico de intereses que se ha presentado anteriormente.

Señala este precepto que, más allá de lo que afecte a la cesión de datos, la regulación de la protección de los datos de carácter personal en el campo de la sanidad se llevará a cabo de acuerdo a la normativa sanitaria, tanto estatal como autonómica. La LOPD ha cambiado, se entiende aquí que para bien, la letra de la LORTAD en este punto. Esta última remitía la regulación de la protección de datos en el ámbito sanitario a una lista concreta de normas, que parecían limitar el marco jurídico a aplicar[391], con el riesgo que ello podía conllevar de dejar fuera de dicho marco otras normas de interés. La remisión en la actualidad es genérica a la normativa sanitaria[392].

Como primer acercamiento al precepto, hay que valorar positivamente el hecho de que se realice una referencia expresa en la Ley al ámbito sanitario, pues denota la preocupación del

ordenador a cambio de una barra de chocolate, y sus datos personales a cambio de participar en un sorteo de dos entradas para el teatro. Noticia publicada en *El Mundo*, de 10 de abril de 2005.

[388] Recomendación (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados Miembros sobre Protección de Datos Médicos.

[389] Artículo 7.3 LOPD: *"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente"*.
Artículo 7.6 LOPD: *"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto"*

[390] Artículo 8 LOPD: *"Datos relativos a la salud.- Sin perjuicio de lo que se dispone en el articulo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica"*.

[391] La remisión la realiza a lo dispuesto en los artículos 8, 10, 23 y 61 de la LGS; 85.5, 96 y 98 de la Ley 25/1990, de 20 de diciembre, del Medicamento; 2, 3 y 4 de la Ley Orgánica 3/1986, de 14 de abril, de medidas especiales en materia de Salud Pública, y demás leyes sanitarias.

[392] ÁLVAREZ CIENFUEGOS, "La aplicación...", cit., 2001, p. 4.

legislador por este tipo de tratamientos[393]. Es más, la idea de remitir la regulación de los datos sanitarios a una norma concreta constituye una fórmula totalmente válida que la propia Ley recoge para otro tipo de datos[394]. El problema radica en la redacción empleada[395].

Más allá de la confusión que genera la referencia al artículo 11 de la Ley, que más adelante se analizará[396], la remisión hubiera tenido pleno sentido si hubiese una norma dedicada a regular específicamente los problemas que plantea el tratamiento de los datos en el ámbito sanitario. Sin embargo, la realidad es bien diferente y ni mucho menos se puede afirmar que normas que regulan el sector como la LGS, Ley del Medicamento, leyes de carácter sectorial como la de Reproducción Asistida, llenan el vacío creado por la inexistencia de la citada norma. Tanto la propia AEPD como gran parte de la doctrina han reconocido que la remisión del artículo 8 de la LOPD es una remisión "vacía" de contenido[397]. A este problema hay que sumar el hecho de que el marco jurídico regulador de la materia sanitaria está compuesto por una infinidad de normas. La dispersión normativa no favorece la seguridad jurídica[398]. Como colofón, en la normativa sanitaria son muchas las remisiones que se hacen a la propia LOPD[399], lo cual da una idea de la laguna que existe en esta rama del Derecho con respecto a este punto. En definitiva, se puede observar que el marco jurídico que resulta de la lectura del citado artículo 8 de la LOPD no presenta unos criterios bien definidos a la hora de resolver los conflictos jurídicos que puedan derivar de las confrontaciones entre los intereses que arriba se han apuntado.

La aprobación de la LBAP, vino a poner algo de luz sobre las sombras[400]. Aún así, tampoco se puede considerar esta norma como receptora de la remisión realizada por el artículo 8 de la LOPD, pues, aunque se refiere a varios aspectos concernientes a los problemas creados en torno a la manipulación de la información clínica, no constituye un marco jurídico completo que regule todas las operaciones que componen el tratamiento de los datos sanitarios[401]. Es bastante significativo en este sentido que la propia LBAP realice remisiones a la LOPD[402].

---

[393] SEOANE RODRÍGUEZ, "De la Intimidad...", cit., 2002, p. 155, subraya que los datos sanitarios son "los únicos datos sensibles enunciados en el art. 7 que merecen un artículo monográfico".

[394] Artículo 2.3 LOPD.

[395] HEREDERO HIGUERAS, "La Protección...", cit., 1999, p. 95, ha llegado a concluir tajantemente que "el artículo 8 de la ley vigente (en referencia a la LORTAD) podría ser suprimido, dada su imprecisión y su redundancia".

[396] De una lectura literal del artículo 8 LOPD se podría deducir que a los datos sanitarios les es aplicable el artículo 11 de la Ley, concerniente a la cesión de datos, pero que más allá de esta disposición se aplicará la legislación sanitaria y no la LOPD. Así, se podría llegar a la conclusión de que en el ámbito sanitario no son alegables, por ejemplo, los principios de calidad recogidos en el artículo 4, o el principio de información reconocido en el artículo 5 de la Ley, relativo al derecho de información. No parece que tenga sentido la exclusión de los datos sanitarios de la aplicación de principios tan fundamentales como los citados. HEREDERO HIGUERAS, *La Ley...*, cit., 1996, p. 107, señala que si la voluntad del legislador hubiera sido la de excluir los datos sanitarios de la aplicación de esos principios básicos, "habría debido decirlo expresamente".

[397] RIPOL CARULLA, "El Tratamiento...", cit., 1999, p. 153.

[398] FERNÁNDEZ LÓPEZ, ex-director de la Agencia de Protección de Datos, *Diariomédico* 7 de septiembre de 2002, en http://www.diariomedico.com, denunció que "la dispersión de la normativa en materia de protección de datos en el ámbito sanitario perjudica al paciente, ya que su aplicación resulta muy difícil".

[399] MARTÍNEZ-CAMPELLO "La Ley 41/2002…", cit., 2004, pp. 219-223.

[400] TRONCOSO REIGADA, "*La protección de datos*...", cit., 2008, p. 31.

[401] Hay autores que han visto en la citada Ley 41/2002, de 14 de noviembre, la norma que definitivamente viene a llenar el vacío que venimos denunciando. En este sentido parecen pronunciarse por ejemplo DE MIGUEL SÁNCHEZ, *Tratamiento de Datos...,* cit., 2004, p. 24, cuando afirma que la citada norma"ha venido a cubrir una importante laguna generadora de gran inseguridad jurídica"; y REBOLLO DELGADO, *Derechos Fundamentales*..., cit., 2004, p. 85, que

Hace ya tiempo que se viene subrayando la idea de que a la hora de regular la protección de los datos sanitarios el ordenamiento presenta serias deficiencias.[403]. La necesidad de una Ley que regule esta materia sigue teniendo hoy día plena vigencia[404].

II.2. Determinación orientativa del marco jurídico que regula la colisión entre el derecho a la autodeterminación informativa y el derecho a la protección de la salud.

Más allá de la aplicación de la LOPD, las normas a tener en cuenta son numerosas. Aún a sabiendas del riesgo que conlleva la elaboración de una lista con las normas que componen el marco jurídico a aplicar en la regulación de la materia que se trata, se establece aquí un listado básico-orientativo con los documentos que principalmente se van a emplear en este trabajo[405].

En el marco de la UE hay que tomar en consideración fundamentalmente la Directiva 95/46/CE y los documentos emitidos por el Grupo de Expertos del artículo 29 de la Directiva[406], que aclaran diferentes puntos de la Directiva ayudando a comprender su contenido. En el ámbito del Consejo de Europa se atenderá al Convenio nº 108 de 1981, de 28 de enero, del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal y a la Recomendación (97) 5, de 17 de febrero de 1997, sobre la protección de datos médicos. Al igual que las demás recomendaciones emitidas por este organismo[407], esta última recomendación, que será de constante cita en el presente trabajo, no tiene efectos jurídicos vinculantes directos para los estados; sin embargo, constituye un *soft law*[408] que deberá ser tenido en cuenta a la hora de interpretar el contenido de las principales normas que serán objeto de análisis, fundamentalmente la LOPD y la Directiva europea de protección de datos.

En el ámbito estatal hay que distinguir entre las normas que regulan la protección de datos y las que regulan el ámbito de la sanidad. Entre las primeras caben destacar la LOPD y el RD

---

igualmente afirma que dicha Ley "viene a paliar las deficiencias existentes en el ámbito de la protección de datos de carácter personal relativos a los pacientes". Frente a esta postura, TRONCOSO REIGADA, *Guía de Protección....,* cit., 2004, p. 22, establece un matiz al afirmar que la reciente norma "viene a paliar parcialmente la posible insuficiencia de la Ley Orgánica 15/1999, de 13 de diciembre", y lo mismo se establece en la obra de LEGALIA, *La Protección...*, 2002, p. 46, en la que se considera que si bien hay aspectos que la Ley 41/2002 vendrá a regular, hay otros que quedarán sin resolver.

[402] Artículo 16.3 LBAP.

[403] MORALES PRATS, "Derecho a la Intimidad...", cit., 2001, pp. 141-142. APARICIO SALOM, *Estudio sobre la Ley...,* 2009, p. 317.

[404] La necesidad de una norma dirigida a la protección de datos en el específico ámbito de la sanidad ha sido una reivindicación en la que han convergido la gran mayoría de los especialistas en la materia. CASTELLS ARTECHE, "El Tratamiento...", cit., 1997, p. 574; LÓPEZ DOMÍNGUEZ, "La Información...", cit., 1997, p. 569; CRIADO DEL RÍO, *Aspectos médico-legales...,* 1999, p. 281; SEOANE RODRÍGUEZ, "De la Intimidad...", cit., 2002, p. 156; UMPIERRE, en *Diariomédico* 26 de marzo de 2002, ÁLVAREZ CIENFUEGOS, en *Diariomédico* de 7 de marzo de 2002 y "La Aplicación...", cit., 2001, pp. 4 y 5; APARICIO SALOM, *Estudio sobre la Ley...,* 2009, p. 317, han apoyado la creación de una norma que, de una vez por todas, aclare todos los aspectos del tratamiento de datos sanitarios.

[405] DE LORENZO Y MONTERO, *Protección de datos…,* cit., 2009, realiza un exhaustivo análisis de las normas y decisiones judiciales más relevantes que afectan a la protección de datos sanitarios.

[406] http://www.europa.eu.int/comm/justice_home/fsj/privacy/

[407] SIERRA NAVA, *El Consejo de Europa…*, cit., 1957, p. 67; SALINAS ALCEGA, *El Consejo de Europa…*, cit., 1999, p. 40, analiza las características de las Recomendaciones aprobadas por el Consejo de Europa.

[408] SENDEN, *Soft Law in European…*, cit., 2004, p. 111, define el *soft law* como las reglas de conducta que se recogen en instrumentos a los que no se atribuyen efectos jurídicos, pero que tienen ciertos efectos indirectos en la práctica.

1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la LOPD, y las recomendaciones, informes jurídicos, memorias, resoluciones e instrucciones de la AEPD, que concretan diversos aspectos de la citada normativa básica[409]. Entre las segundas hay que atender a normas de alcance general, caso de la Ley General de Sanidad 14/1986, Ley 16/2003, de 28 de mayo de Cohesión y Calidad del Sistema Nacional de Salud, Ley 44/2003, 21 de noviembre, de ordenación de las profesiones sanitarias, Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública, y a normas que regulan aspectos más concretos de la actividad sanitaria como la importante Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica, la Ley 14/2007, de 3 de julio de Investigación Biomédica, la Ley 14/2006, 26 de mayo, sobre Técnicas de Reproducción Humana Asistida, la Ley 30/1979, de 27 de octubre, sobre Trasplante de Órganos, la Ley 29/2006, 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios o el RD 1718/2010, de 17 de diciembre, sobre Receta Médica y Ordenes de Dispensación..

En el ámbito autonómico se puede hacer la misma distinción. Entre las normas que regulan la protección de datos hay que destacar la Ley Catalana 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos; la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid; la Ley Vasca 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal y de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos; y los informes y las recomendaciones de las Agencias de Protección de Datos Autonómicas[410]. Entre las que regulan el ámbito sanitario cabe subrayar la Ley Foral 17/2010, 8 de noviembre, de Derechos y Deberes de las Personas en Materia de Salud en la Comunidad Foral de Navarra, la Ley Catalana 21/2000, de 29 de diciembre, sobre los Derechos de Información Concerniente a la Salud y a la Autonomía del Paciente, y la Documentación Clínica, o el Decreto del País Vasco 45/1998, de 17 de marzo, por el que se establece el Contenido y se regula la Valoración, Conservación y Expurgo de los Documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias, o recientes normas autonómicas reguladoras de materias más concretas, caso del Decreto 29/2009, 5 de febrero, por el que se regula el Uso y Acceso a la Historia Clínica Electrónica de Galicia, o de la Resolución de 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam (Servicio de Salud de Castilla-La Mancha), o del Decreto 181/2007, 19 de junio, por el que se regula la Receta Médica Electrónica en Andalucía.

Además de las normas citadas, a la hora de dar solución a los diferentes problemas que se vayan planteando en la manipulación de datos de carácter personal en el ámbito sanitario, habrá que tener en cuenta también otros textos que desde el propio sector se han aprobado con la finalidad de regular esta materia en centros o sistemas sanitarios concretos[411], tanto públicos

[409] Agencia Española de Protección de Datos (AEPD), http://www.agpd.es/.

[410] Agencia Vasca de Protección de Datos (AVPD) http://www.avpd.euskadi.net/; Agencia Catalana de Protección de Datos (ACPD) http://www.apdcat.net/; Agencia de Protección de Datos de la Comunidad de Madrid (APDCM) http://www.madrid.org/apdcm/.

[411] RUBÍ NAVARRETE, "Los Códigos...", cit., 2000, pp. 1-5; RUBÍ NAVARRETE, "Códigos Tipo…", cit., 2009, p. 167, para profundizar en los problemas que plantea el sistema de la "autorregulación".

como privados[412]. Se está haciendo referencia a los instrumentos de autorregulación como protocolos de actuación o códigos tipo, que si bien tienen aplicación en el ámbito puramente interno de centros o sistemas sanitarios concretos, adquieren gran relevancia en la medida en que fijan una forma de actuación con respecto a la forma de manipular la información de carácter personal[413]. Hace tiempo que se subrayó la importancia de estos instrumentos normativos[414]. Se trata de mecanismos que, a pesar de que en la actualidad no cuenten con un gran desarrollo, cada vez obtienen mayor reconocimiento[415] y ya se están elaborando en diferentes sectores[416].

No se está haciendo referencia ahora a los Códigos Deontológicos como el Código de Ética y Deontología Médica, que conciernen ante todo al comportamiento ético de los profesionales, sino a disposiciones de carácter técnico que recogen los aspectos más concretos de la regulación de la protección de datos de carácter personal en un centro o sistema sanitario. Esta forma de actuación adquiere en la actualidad relevancia jurídica en el ámbito de la protección de datos en el artículo 32 de la LOPD[417]. Lo dispuesto en la Ley se desarrolla en el RDLOPD, que concreta el

[412] ULL PONT, *Derecho público...*, cit., 2000, p. 132, critica la ubicación del artículo 32 de la LOPD, pues se sitúa en el apartado correspondiente a los ficheros privados, cuando los códigos pueden afectar tanto a ficheros privados como a públicos, cosa que no ocurría en la LORTAD.

[413] MARTÍN PARDO, "Los códigos tipo…", cit., 2005; HELGUERO SAINZ, "Objeto y naturaleza…", cit., 2010, p. 1.728.

[414] Grupo de Expertos en Información y Documentación Clínica, documento final de 26 de noviembre de 1997, señala que estos protocolos son absolutamente necesarios pues "permiten orientar a los profesionales sanitarios en su quehacer diario; teniendo en cuenta las peculiaridades de cada centro y aun las circunstancias de cada paciente"

[415] Es significativo ver como las normas que en la actualidad se dedican a regular el sector sanitario hacen mención, cada vez con mayor frecuencia, a estos mecanismos jurídicos. En este sentido el artículo 4.7 de la Ley 44/2003, de 21 de noviembre, de Ordenación de las Profesiones Sanitarias apunta que "*El ejercicio de las profesiones sanitarias se llevará a cabo con plena autonomía técnica y científica, sin más limitaciones que las establecidas en esta ley y por los demás principios y valores contenidos en el ordenamiento jurídico y deontológico y de acuerdo con los siguientes principios:*

b)Se tenderá a la unificación de los criterios de actuación, que están basados en la evidencia científica y en los medios disponibles y soportados en guías y protocolos de práctica clínica y asistencial. Los protocolos deberán ser utilizados de forma orientativa, como guía de decisión parar todos los profesionales de un equipo y serán regularmente actualizados con la participación de aquellos que los deban aplicar". CAZURRO BARAHONDA, "Objeto y naturaleza…", cit., 2010, p. 1.747.

[416] Cabe citar como ejemplos más significativos, el Código Tipo de la "Asociación Catalana de Recursos Asistenciales (ACRA), y el de la "Agrupación Catalana de Establecimientos Sanitarios". Instrucción 6/2003, del Director General de Osakidetza sobre las funciones y obligaciones del personal de Osakidetza con relación a la protección de datos de carácter personal, 2 de septiembre de 2003. Circular 9/1997, de 9 de julio de 1997, del INSALUD, sobre Instrucciones sobre Seguridad y Protección de Datos.

[417] Artículo 32 LOPD, atendiendo al artículo 27 de la Directiva europea: "*Códigos Tipo*. *1-Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupan, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.*

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológico o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la

contenido que han de tener estos códigos y el procedimiento a seguir en su aprobación[418]. En la normativa sanitaria, las leyes instan a las administraciones sanitarias a aprobar estos protocolos[419].

Este tipo de regulación constituye un tercer eslabón en la reglamentación de la protección de los datos de carácter personal sanitarios, que completa en la práctica la regulación propuesta por la LOPD[420]. De alguna manera, estos protocolos de actuación configuran un *soft law* que adecua la normación genérica de la Ley a las características concretas de los diferentes centros o sistemas sanitarios. Como señalaba la Exposición de Motivos de la LORTAD, se trata de un mecanismo jurídico muy adecuado para ese fin pues constituye un instrumento flexible y de rápida elaboración, muy pertinente para recoger matices. A pesar de que la exigibilidad de su cumplimiento puede ser cuestionable[421], estos mecanismos pueden servir para llenar el vacío jurídico que crea en el ámbito estatal la inexistencia de una Ley que regule la protección de datos de carácter personal en el ámbito sanitario[422].

A falta de una norma concreta que regule en el ámbito interno la protección de los de carácter personal en el sector sanitario, la solución a los problemas jurídicos que resulten de la necesidad de cohonestar la autodeterminación informativa de las personas y el apremio de manipular información de carácter personal derivará fundamentalmente de la interpretación del marco jurídico expuesto.

Como se ha dicho, a la hora de realizar este ejercicio de interpretación no parece adecuado tomar como referencia posiciones particularmente radicales que tengan una visión teórica, muchas veces preconcebida, sobre el papel que las nuevas tecnologías han de tener en la sociedad y, concretamente, en el ámbito de la salud. Las posturas especialmente garantistas pueden llevar a cerrar las puertas a alternativas plenamente válidas que favorecen el tratamiento sanitario de las personas[423]. Y al revés, posturas particularmente permisivas con el uso de dichas tecnologías pueden llegar a vaciar de contenido los derechos a la intimidad y a la autodeterminación informativa, lo cual, hay que decirlo, acabaría afectando al buen

materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos, requerir a los solicitantes para que efectúen las correcciones oportunas"

[418] Artículos 71 a 78 RDLOPD.

[419] Artículo 31.2 Ley Foral 17/2010, 8 de noviembre, de Derechos y Deberes de las Personas en materia de Salud en la Comunidad Foral de Navarra: "*La administración sanitaria navarra y los centros sanitarios deben adoptar las medidas oportunas para garantizar los derechos a que se refiere el apartado 1, elaborando, en su caso, normas y protocolos para garantizar la legitimidad del acceso a los datos de los pacientes. En tal caso deberán comunicarse a los usuarios las razones y el modo de proporcionar tales informaciones*".

[420] Memoria de la AEPD de 2008, donde se apunta la importancia de estos instrumentos como complementos del marco normativo, que ayudan a dar una mayor seguridad jurídica, fijando aspectos concretos de cómo se ha de aplicar dicho marco normativo en ámbitos determinados.

[421] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 363; HELGUERO SAINZ, "Objeto y naturaleza…", cit., 2010, p. 1.730, señala que la obligatoriedad del contenido de los códigos tipo se impondrá a quienes se hayan adherido al mismo, pero no son, *per se,* normas jurídicas vinculantes.

[422] RUBÍ NAVARRETE, "La Protección...", cit., 2003, apuntó también la posibilidad de emplear estos instrumentos jurídicos como mecanismos para suplir la falta de regulación específica y complementar así la LOPD; HELGUERO SAINZ, "Objeto y naturaleza…", cit., 2010, p. 1.728; CAZURRO BARAHONA, "Objeto y naturaleza…", cit., 2010, p. 1.764.

[423] DE MIGUEL SÁNCHEZ, *Secreto médico…*, cit., 2002, p. 292, refleja las voces de investigadores que señalan que una excesiva protección de los datos puede tener una incidencia negativa para el desarrollo científico.

funcionamiento de los sistemas sanitarios que se basan, ente otras cosas, en la institución de la relación de confianza entre profesionales y usuarios, que exige a los primeros actuar respetando la obligación de secreto.

La interpretación de este marco jurídico, sobre todo cuando se trata de limitar un derecho fundamental, deberá hacerse teniendo en cuenta las coordenadas que arriba se han dado, es decir, atendiendo en cada supuesto a la importancia que pueda tener el fin que se persigue con la manipulación de los datos de carácter personal: salvar una vida, realizar un estudio epidemiológico, llevar a cabo un control económico en la gestión de la Administración sanitaria, etc., y en qué medida afecta dicha actuación al derecho a la autodeterminación informativa: si se trata de información especialmente sensible como puede ser la afección del VIH, etc.

III. LA APLICABILIDAD DE LA LOPD A LOS TRATAMIENTOS NO AUTOMATIZADOS.

III.1. La importancia de reconocer la aplicabilidad de las normas dirigidas a proteger los datos de carácter personal a los tratamientos manuales.

Otra de las cuestiones que, previamente al estudio de los aspectos más relevantes del contenido del derecho a la autodeterminación informativa aplicado al sector sanitario, hay que analizar, es la aplicabilidad de la LOPD a los tratamientos de datos no automatizados. Se ha indicado repetidas veces que precisamente éste es uno de los aspectos en que la LOPD ha supuesto un mayor cambio con respecto a la LORTAD. Mientras que esta última se aplicaba sólo a los ficheros automatizados, la LOPD abraza también a los manuales[424]. Hay que desarrollar ahora, aunque sea brevemente, este punto por la especial relevancia que adquiere en el ámbito sanitario.

En la actualidad, prácticamente todas las normas que regulan con carácter general la protección de datos de carácter personal se aplican tanto a ficheros automatizados como a manuales. Sin embargo esto no siempre ha sido así. El Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, como su propio nombre indica, se refiere sólo a los ficheros automatizados. Dicho Convenio parte de la consideración de que el empleo de las nuevas tecnologías supone un mayor riesgo en la manipulación de ficheros que el tradicional uso manual de los mismos. Consecuentemente, se trata de una norma que, como la memoria explicativa del mismo señala, tiene por objeto la protección de la persona ante el fuerte y rápido desarrollo de estas nuevas

[424] Artículo 2 LOPD: "*Ámbito de aplicación.-1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado".* Y en el artículo 3 de la misma Ley se define el concepto de fichero como *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso",* y el concepto de tratamiento como *"operaciones y procedimientos técnicos de carácter automatizado o no (...)".* Tanto la Ley de la Comunidad de Madrid, la catalana como la vasca, se pronuncian en el mismo sentido.

tecnologías, planteando así como ámbito de aplicación sólo los ficheros automatizados y dejando a un lado los que son objeto de un uso manual[425].

La LORTAD, atendiendo a este Convenio y, sobre todo, al contenido del artículo 18.4 CE, mantuvo el mismo criterio. Si se observa su Exposición de Motivos se encontrará que las TIC son consideradas como un riesgo para lo que en esta Ley se denomina "privacidad" de las personas. Así pues, y tal como se puso de manifiesto por la jurisprudencia, el ámbito de aplicación de la norma se limitaba a los ficheros automatizados[426]. Aún así no hay que pasar por alto la posibilidad que abría la Ley al habilitar al Gobierno para que, previo informe del Director de la Agencia de Protección de Datos, extendiese lo dispuesto en la norma, con las correspondientes adecuaciones, a los ficheros manuales[427].

La aprobación en el ámbito de la UE de la Directiva 95/46/CE constituye un punto de inflexión en relación a esta cuestión. El ámbito de aplicación de esta norma abraza tanto a los ficheros automatizados como a los manuales. Hubo países que se negaron a la inclusión de estos últimos en el ámbito de aplicación de la Directiva[428], pero afortunadamente en última instancia se aprobó dicha incorporación. Lo fundamental no es limitar el desarrollo de las nuevas tecnologías, sino la protección de los datos de carácter personal, independientemente del formato en que éstos se encuentren. El riesgo de que el derecho a la autodeterminación informativa se vea vulnerado por el tratamiento manual de datos se tiene en consideración en la Directiva[429]. En esta norma no se pone el acento tanto en el desarrollo de la tecnología, sino en la necesidad de proteger a los individuos de los posibles ataques a su autodeterminación informativa, vengan de donde vengan[430].

---

[425] Artículo 1 Convenio 108/1981 del Consejo de Europa. Memoria Explicativa del Convenio 108/1981 del Consejo de Europa: "*El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida"*

[426] Artículo 2 LORTAD: *"Ámbito de aplicación. 1. La presente Ley será de aplicación a los datos de carácter personal que figuran en ficheros automatizados de los sectores públicos y privados y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado"*. Como apunta la SAN de 25 de mayo de 2001 de la Sala de lo Contencioso Administrativo, la "finalidad de hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos, provoca que la ley se centre en torno a los denominados ficheros de datos, introduciendo el término fichero "tratamiento automatizado" de los mismos".

[427] Disposición Final segunda LORTAD.

[428] HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 130. Gran Bretaña, Irlanda y Dinamarca consideraban que la manipulación manual de los datos de carácter personal no constituían un riesgo comparable al que suponía la informática, por lo que se oponían a la inclusión de este tipo de tratamiento en el ámbito de aplicación de la Directiva.

[429] Considerando nº 27 Directiva 95/46/CE: "*(...) el alcance de esta protección no debe depender, en efecto, de las técnicas utilizadas, pues lo contrario daría lugar a riesgos graves de alusión (...)*". Artículo 3.1 Directiva 95/46/CE: "*Las disposiciones de la presente Directiva se aplicarán al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*".

[430] En el caso de la Directiva, la necesidad de que la protección se expandiese también a los ficheros manuales era evidente, pues la finalidad de posibilitar la circulación de los datos de carácter personal por todo el territorio comunitario hacía necesario que la protección de dichos datos se diese tanto cuando éstos se situasen en soporte informático como cuando se situasen en soporte manual. VILLAR ROJAS, "El Nuevo...", cit., 2000, p. 157, afirma que el fundamento de la Directiva no es otro que el establecimiento de las condiciones adecuadas para posibilitar la circulación de los datos, por lo que es necesario que se establezca un mínimo de protección en todos los ficheros.

La LOPD, siendo la transposición de la Directiva, no podía recoger una regulación diferente a la planteada por la norma comunitaria, por lo que hace suyo el planteamiento de la misma. Así, se suprime de la vigente Ley el adjetivo de "automatizado", que acompañaba en el articulado de la LORTAD al concepto de fichero[431], quedando claro que la norma se aplicará tanto a ficheros automatizados como a manuales. El reglamento que desarrolla la Ley recoge la misma fórmula[432].

La Recomendación del Consejo de Europa sobre la protección de datos médicos se aplica a los tratamientos automatizados; sin embargo, abre la puerta para que los estados extiendan su contenido a los datos no procesados automatizadamente[433]. Como es lógico, aplicándose la LOPD tanto a tratamientos automatizados como manuales, parece evidente que el contenido de la citada Recomendación hay que entenderlo aplicable en la misma medida para ambos casos.

La importancia de incluir en el ámbito de aplicación de estas normas los tratamientos manuales de datos resulta evidente. Podía resultar comprensible que las normas de primera generación dedicadas a la protección de los datos de carácter personal se centraran en la necesidad de limitar y fiscalizar el uso de las TIC. La facultad de controlar las manipulaciones que de los datos de cada uno se podían realizar se asociaba con el peligro que las nuevas tecnologías conllevaban para el efectivo ejercicio de este derecho. Hoy día, sin embargo, con la consagración del derecho a la autodeterminación informativa como derecho fundamental, se entiende que la facultad de controlar los usos que se puedan dar a los datos que conciernen a las personas ha de alcanzar a todo tipo de operaciones, independientemente de si se hacen empleando las TIC o no. Si tal derecho tiene como contenido la facultad de controlar los tratamientos que de los datos de cada uno se vayan a llevar a cabo, no parece correcto dejar sin protección a las personas en lo que respecta a sus datos de carácter personal, por el hecho de que éstos no se encuentren automatizados. Si bien es incuestionable que las nuevas tecnologías posibilitan nuevas formas de irrumpir en la vida privada de la ciudadanía, no es menos cierto que la manipulación manual de los ficheros puede acarrear también serios perjuicios en la autodeterminación informativa de las personas[434]. El objetivo inmediato de las normas que regulan la protección de datos tiene que ser regular todo tipo de tratamiento, sea automatizado o no, de los datos de carácter personal[435].

Estando completamente de acuerdo con la consideración de que el tratamiento de todo tipo de ficheros tiene que atender a lo dispuesto en la LOPD, no se puede escapar a la idea de que las

[431] Hay que apuntar que en algunos artículos todavía se emplea el concepto de "fichero automatizado" que parece excluir los ficheros manuales, caso del Artículo 26.3 LOPD. Sin duda, estos casos son fruto del olvido, y no responden a una intención del legislador de excluir los ficheros manuales de la aplicación de los artículos en los que esto ocurre. DEL PESO NAVARRO, "Principales Diferencias...", cit., 2000, p. 12.

[432] Artículo 2.1 RDLOPD.

[433] Artículo 2 R (97) 5: "*1. Esta recomendación es aplicable a la recogida y tratamiento automatizado de datos médicos, salvo que la ley nacional, en un contexto específico fuera del sector sanitario, proporcione otras medidas de seguridad apropiadas. 2. Un Estado miembro puede extender los principios establecidos en esta recomendación a datos médicos no procesados automatizadamente*".

[434] CUERVO, "Autodeterminación Informativa", cit., 1998 afirma que la manipulación manual de los datos de carácter personal "puede suponer un auténtico peligro para la intimidad de las personas; peligros equiparables a los que implica el tratamiento automatizado, donde las evidentes ventajas técnicas que nos ofrece este último, pueden ser suplidas por el enorme potencial humano, p. ej. de las Administraciones Públicas o de las grandes empresas". HEREDERO HIGUERAS, *La directiva...*, cit., 1997, pp. 85-86.

[435] SÁNCHEZ CARAZO, *La intimidad...*, cit., 2000, pp. 41-42.

características de los ficheros manuales son distintas a las de los ficheros automatizados. La aplicación de los principios recogidos en la citada norma, fundamentalmente las medidas de seguridad, tiene mayores dificultades cuando se trata de ficheros manuales. Piénsese, por ejemplo, en el ámbito sanitario, las dificultades de organización que puede llegar a generar la manipulación exclusivamente manual de todas las historias clínicas con las que cuenta un centro de sanidad.

Esta idea se deja entrever en la propia Ley al otorgar un plazo de doce años, a contar a partir del 24 de octubre de 1995, para la aplicación de su contenido a los ficheros y tratamientos no automatizados que existían antes de la entrada en vigor de la LOPD[436]. Se dejaba un amplio margen de tiempo para que los responsables de los ficheros manuales pudieran tomar todas las medidas oportunas para que dichas bases de datos respetasen los principios recogidos en la Ley. Esto no quería decir que en este intervalo de tiempo los titulares de los datos contenidos en esos ficheros no pudieran ejercer sus derechos. Como bien ha señalado la jurisprudencia en alguna ocasión, esta prórroga no podía suponer la indefensión en este periodo de tiempo de los ciudadanos con respecto a sus datos de carácter personal[437]. La propia Ley entendía que la prórroga no podía afectar al ejercicio de los derechos de acceso, rectificación y cancelación, que, por lo tanto, podían ejercerse también con respecto a ficheros manuales. Se considera aquí que la inmediatez en la aplicación de la LOPD a los ficheros manuales no se podía limitar a los citados derechos, sino que tenía que ampliarse a principios como los referidos a la calidad de los datos, la información o el consentimiento, pues no tenía sentido que se aceptaran los derechos de acceso, rectificación y cancelación sin que se reconociera, por ejemplo, el derecho a la información[438].

La principal dificultad a la hora de aplicar la LOPD a los ficheros manuales se presenta en el momento en que se quieren adoptar las medidas de seguridad a las que se refiere la Ley en dichas bases de datos. Antes de la entrada en vigor del actual reglamento que desarrolla la LOPD (RDLOPD), el reglamento que regulaba las medidas de seguridad, RD 994/1999, de 11 de junio, no hacía distinción alguna entre ficheros automatizados y manuales. Esto era así debido a que dicho reglamento desarrollaba la LORTAD, que se refería exclusivamente a los ficheros automatizados. Teniendo en cuenta que dicho reglamento ha estado vigente hasta el 2007, que es cuando se ha aprobado el actual, no es difícil imaginar los problemas prácticos que han derivado de la necesidad de cohonestar la LOPD y el reglamento de 1999. No podía entenderse que dicho reglamento, creado pensando en los ficheros automatizados, fuera aplicable sin matices a los ficheros manuales[439]. Hay que recordar que el incumplimiento de estas medidas de

[436] Disposición Adicional primera, LOPD.

[437] SAN de 19 de mayo de 2004, FJ 4, afirma con respecto al citado plazo de doce años para los ficheros manuales, que "no puede sostenerse válidamente que se establezcan vacaciones tan prolongadas con respecto en el cumplimiento de unos deberes en el que pueden resultar gravemente afectados derechos fundamentales de las personas".

[438] SAN de 19 de mayo de 2004, FJ 4, reconoce que "las previsiones de la Ley Orgánica 15/1999 (...), que garantizan y protegen, en lo concerniente al tratamiento de los datos personales, los derechos fundamentales y las libertades públicas de las personas físicas, y, especialmente su derecho al honor y a la intimidad personal y familiar, han de aplicarse inmediatamente, en virtud del principio de aplicabilidad inmediata de los derechos fundamentales, según doctrina del Tribunal Constitucional recogida en la sentencia 81/1992, de 28 de mayo".

[439] TRONCOSO REIGADA, *Guía de Protección...*, 2004, cit., p. 55, subraya que una "cosa es que la vigencia de unas medidas de seguridad organizativas previstas en el Reglamento de Medidas de Seguridad pueda *recomendarse* también en el ámbito de los ficheros no informatizados, y otra que se pueda exigir jurídicamente y que pueda sustanciar esta inobservancia una resolución de infracción".

seguridad acarreaba duras sanciones. Hoy día este problema queda resuelto en el nuevo reglamento, en la medida en que prevé medidas específicas dirigidas a los ficheros manuales[440].

La idea de que todo tipo de ficheros se encuentre en el ámbito de aplicación de la LOPD adquiere una especial relevancia en el sector sanitario. Hay que tener en cuenta que en este entorno es muy alto el número de ficheros manuales que, todavía hoy, se manipula diariamente[441]. La automatización de las historias clínicas es un proceso más bien lento, y ello hace que en muchos lugares se sigan empleando las historias clínicas tradicionales. En el capítulo anterior se veían las ventajas e inconvenientes del uso de las nuevas tecnologías con respecto al papel en el ámbito sanitario, y se apuntaba que en el traslado de los documentos en formato papel, en su puesta al día, en el acceso por parte de los diferentes profesionales a los mismos, etc., se crean situaciones de verdadero riesgo para los derechos de los pacientes, incluso mayores que los planteados por el uso informático de los mismos. Piénsese en la frecuencia con la que se traspapelan o se pierden los documentos que componen las historias. Tratar de asumir que a estos ficheros no les es de aplicación la normativa de protección de datos constituiría una equivocación[442]. Los principios básicos que rigen el tratamiento de datos de carácter personal, los derechos de acceso, cancelación, rectificación y oposición, las obligaciones que corresponden a los diferentes sujetos implicados en la manipulación de los datos de carácter personal sanitarios, necesariamente tienen que aplicarse a las historias clínicas no informatizadas y a los demás ficheros que recojan los datos de los pacientes. Lo contrario situaría a éstos en una situación de absoluta indefensión, que no se corresponde con lo que predica el principio de autonomía que hoy día preside la relación médico-paciente, pues negaría al paciente el control que le corresponde sobre sus datos.

III.2. La necesidad de que los datos sean o vayan a ser incluidos en un fichero para que la Ley pueda aplicarse a los tratamientos manuales de los datos.

Se acaba de ver que el ordenamiento protege el derecho a la autodeterminación informativa cuando el tratamiento de los datos se produce empleando medios no automatizados. Este criterio está plenamente justificado por cuanto dicho derecho puede verse también afectado cuando no se utilizan las TIC para manipular la información. La aplicabilidad de las normas al tratamiento manual de los datos está sujeta, sin embargo, a condiciones.

La Directiva europea señala expresamente que el régimen jurídico en ella dispuesto es aplicable a los tratamientos manuales de datos, siempre y cuando estén contenidos o destinados

[440] Artículo 105 y siguientes RDLOPD.

[441] Memoria de la AEPD del 2002, p. 47, en la que se pone de manifiesto que el ámbito sanitario es el que más ficheros manuales ha dado de alta.

[442] ORTÍ VALLEJO, *Derecho a la Intimidad...,* cit., 1994, p. 83, basándose en las palabras de la <<*Comisión national de l´informatique et des libertés*>>, afirma que "los ficheros manuales presentan más amenazas para la vida privada y las libertades, pues cuando se componen de centenares de miles o incluso de millones de fichas, su puesta al día no es posible, con lo cual se mantendrían inexactitudes en los datos personales". Además, señala el autor que los "ficheros automatizados frente a los manuales tienen la ventaja de poder ser destruidos fácilmente y ser susceptibles de medidas de seguridad más eficaces para hacerlos confidenciales". Estas palabras cobran indudablemente pleno sentido en el ámbito sanitario.

a ser incluidos en un fichero[443]. Apunta, además, que su contenido no se aplica a las carpetas que no estén estructuradas, exigiendo, a su vez, que la estructuración se realice de acuerdo a criterios relativos a las personas, que permitan acceder fácilmente a los datos personales[444]. Para que la Directiva se aplique a un tratamiento manual será necesario, por lo tanto, que se trate de datos que provengan o tengan como destino un fichero, público o privado, y que además dicho fichero se estructure en base a criterios personales que hagan que sea fácil el acceso a los datos. La LOPD no contiene tal regulación. Dispone, simplemente, que la Ley se aplicará a los datos registrados en soporte físico que los haga susceptibles de tratamiento[445] y otorga una definición del concepto fichero, entendiéndolo como "*conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso*"[446]. El reglamento que desarrolla la Ley afina más y entra a definir los ficheros no automatizados como "*todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica*"[447]. Se da a entender que el tratamiento manual de datos que no se incluya en el marco determinado por esta definición queda fuera del ámbito de aplicación del reglamento[448].

La falta de referencia expresa en la Ley a su aplicabilidad a los tratamientos manuales ha generado cierta polémica sobre las condiciones que han de cumplirse para que este tipo de manipulaciones se incluyan también en el ámbito de aplicación de la LOPD. Hay diferentes interpretaciones posibles. En primer lugar, en la medida en que la Ley no recoge exigencias concretas, podría entenderse que amplía su ámbito de aplicación más allá de lo dispuesto por la Directiva, a todo tipo de tratamiento manual, independientemente de si se encuentra o no en un fichero estructurado de una manera determinada. Tanto la jurisprudencia como la doctrina se han planteado en algún momento esta posibilidad[449]. En segundo lugar, teniendo en cuenta que la Ley exige que los datos estén en soporte físico que los haga susceptibles de tratamiento, se ha entendido en algún caso, tanto por la doctrina[450] como la jurisprudencia[451], que la referencia al soporte físico constituye el requerimiento de un fichero. De esta forma podría parecer que la Ley

[443] Artículo 3.1 Directiva 95/46/CE.
[444] Considerandos 15 y 27 Directiva 95/46/CE. PUENTE ESCOBAR, "Ámbito objetivo…", cit., 2008, p. 48.
[445] Artículo 2.1 LOPD.
[446] Artículo 3.b) LOPD, que viene a hacer suya la definición de la Directiva europea: artículo 2.c): "*Fichero de datos personales: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica*". Informe jurídico AEPD, 0476/2008, entiende que para considerar que hay un fichero es necesario que se puedan identificar una estructura básica y la descripción de los tipos de datos de carácter personal incluidos en el mismo, y la finalidad para la que se emplee sea identificable.
[447] Artículo 5.1. n) RDLOPD.
[448] FATÁS y GARCÍA SANZ, "Título Primero…", cit., 2008, p. 95.
[449] SAN 18 de diciembre de 2006, FJ 4. LESMES SERRANO, "Artículo 2…", cit., 2008, p. 70.
[450] LESMES SERRANO, "Artículo 2…", cit., 2008, p. 72.
[451] STS 18 de diciembre de 2006, FJ 4: "(…) Es claro para este Tribunal que registro en soporte físico equivale a fichero en los términos de la Ley"; STS 13 de marzo de 2009, FJ 2, en la que se entiende que unos números de teléfono vinculados a personas no constituyen datos de carácter personal a efectos de aplicar la LOPD en la medida en que no se encuentran incluidos en un sistema organizado.

exige para su aplicación, que los datos se encuentren en un fichero, independientemente de que la manipulación sea manual o automatizada.

De lo que dictan las normas citadas se realiza aquí la siguiente interpretación. En relación a los tratamientos automatizados no parece que pueda haber duda sobre la aceptación de un criterio amplio. Se aplica la Ley a todo tipo de tratamiento automatizado, sin que sea necesario que la manipulación afecte a datos incluidos o destinados a incluirse en un fichero estructurado de una determinada manera, siempre que dichos datos se encuentren incorporados en un soporte físico. La regulación de la Directiva parece clara a este respecto. En la norma europea la referencia al fichero se hace en relación a la manipulación manual, pero no cuando se refiere a los tratamientos automatizados. En este último caso la Directiva se aplicará independientemente de si los datos se van a vincular a un fichero estructurado. Favorece esta interpretación la comparación entre el contenido de la LORTAD y de la LOPD. La primera extendía su ámbito de aplicación a los datos contenidos en "*ficheros automatizados*". La existencia de un fichero resultaba esencial para considerar aplicable la norma a los tratamientos automatizados. La LOPD no incluye esa expresión y se refiere a los datos "*registrados en soporte físico*". Desaparece aquí la referencia al fichero, por lo que se puede interpretar que la aplicabilidad de la Ley no depende, en todo caso, de la existencia de un fichero organizado[452]. En esta línea, los tribunales, a pesar de que recientemente han adoptado decisiones algo confusas a este respecto[453], han aplicado la LOPD a tratamientos automatizados que no tienen como fin la inclusión de los datos en un fichero o que no provienen de un fichero. Se ha entendido que la manipulación de la información por instrumentos automatizados queda sometida plenamente a la normativa de protección de datos, sin necesidad de cumplir estrictos requisitos[454], por cuanto que este tipo de tecnología encierra un mayor riesgo de que los datos puedan ser tratados de manera irregular[455]. No hay que olvidar que las técnicas automatizadas, informáticas concretamente, posibilitan siempre las búsquedas de la información.

En relación a los tratamientos manuales, por el contrario, no parece que de la normativa expuesta pueda deducirse una interpretación especialmente amplia de la Ley. La jurisprudencia ha venido siguiendo el criterio definido en la norma europea cuando se ha enfrentado a conflictos generados en torno al tratamiento manual de datos[456]. Diferentes informes jurídicos de la AEPD

[452] DAVARA RODRÍGUEZ, "El concepto de fichero…", cit., 2010, p. 215.

[453] STS 30 de diciembre de 2009, FJ 6 y SAP de Madrid 11 de junio de 2010, FJ 3, en la que parece subrayar la necesidad de que los datos provengan de un fichero estructurado en todo caso, independientemente de que el tratamiento sea manual o automatizado, si bien a efectos de poder aplicar un concreto tipo penal, no tanto para determinar si a dicho tratamiento le es aplicable la normativa de protección de datos: "Los datos, además, han de estar "recogidos (registrados) en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Fichero es todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (art. 3 b. LPDP)".

[454] STJUE 6 de noviembre de 2003, Bodil Lindqvist, asunto C-101/01, FJ 25, reconoce que "la conducta que consiste en hacer referencia, en una página web, a datos personales debe considerarse un tratamiento de esta índole". SAN 24 de enero de 2003, FJ 3, en la que se señala que la captación y transmisión a través de Internet de imágenes capturadas por una cámara constituye un tratamiento a pesar de que dichas imágenes no se vayan a registrar o guardar en fichero alguno.

[455] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007.

[456] SAN 12 de mayo de 2004, FJ 4, señalando que una manipulación de un dato recogido de un tablón, sin que dicha información se haya incluido en fichero alguno no constituye infracción por quien emplea dicho dato. Esta

ponen de manifiesto también que ese criterio ha de ser el aplicado[457]. La norma se aplicará si la manipulación manual afecta a informaciones vinculadas con un fichero concreto estructurado de acuerdo a criterios relativos a la persona[458]. De esta manera, tratamientos no automatizados de los datos, como por ejemplo la apertura de la correspondencia o la inclusión de datos en carpetas desestructuradas o no organizadas quedarían fuera del campo de aplicación de la LOPD[459]. Llevando al extremo la aplicación de este criterio, se ha entendido que ficheros organizados y estructurados en base a parámetros distintos a los personales como puede ser la fecha, obrantes en centros sanitarios y dependencias policiales, no son objeto de aplicación de la LOPD[460].

La asunción de este criterio, que es el reconocido en las normas, fundamentalmente en la Directiva europea, puede plantear problemas de interpretación. Estos conflictos se han dejado ver en la polémica creada en relación a los ficheros bautismales[461]. La consideración de que estos ficheros no cumplían con los requisitos arriba expuestos impidió a los titulares de los datos que los ficheros contenían ejercer los derechos reconocidos en la LOPD[462]. En un inicio, tanto diferentes resoluciones e informes jurídicos de la AEPD[463] como los tribunales[464], otorgaron la consideración

circunstancia puede ser criticable, por cuanto hay un tratamiento claro, que afecta al derecho a la autodeterminación informativa; SSAN 9 de noviembre de 2005, FJ 2 y 26 de noviembre de 2008; SSTS 18 de diciembre de 2006, FJ 4: "(…) para que una actuación manual sobre datos personales (recogida, grabación, conservación, elaboración, modificación, bloqueo…) tenga la consideración de <<tratamiento de datos personales>> sujeto al sistema de protección de la Ley Orgánica 15/1999 es necesario que dichos datos estén contenidos o destinados a ser incluidos en un fichero, esto es, un conjunto estructurado u organizado de datos con arreglo a criterios determinados"; 10 de octubre de 2008.

[457] Informe jurídico AEPD, 0147/2009. Informe jurídico AEPD, 0279/2009, en el que se plantea si una carpeta en formato papel constituye un fichero: basándose en la definición que se da en el RDLOPD art. 5.1.n) se señala que "la ordenación de los documentos por fecha no constituye un fichero, al no estar éste estructurado conforme a criterios relativos a las personas físicas y siempre que impida acceder a los datos personales incorporados en los documentos exija esfuerzos desproporcionados a los datos personales". Resolución de la AEPD R/01797/2008, 15 de enero de 2009. Procedimiento PS/00415/2008, en la que se considera que no hay infracción de la LOPD, porque, a pesar de haberse manipulado cierta información de una persona en formato papel sin el consentimiento del mismo con fines publicitarios, esta información no constaba en fichero alguno. Resolución de la AEPD R/00238/2008, 5 de marzo de 2008. Procedimiento PS/00312/2007, en la que se considera aplicable la LOPD al uso de un dato de salud en una carta de despido.

[458] DAVARA RODRÍGUEZ, "El concepto de fichero…", cit., 2010, p. 213 y siguientes, realiza una interesante reflexión sobre el alcance del concepto de fichero y los problemas interpretativos que plantea. A su vez, marca las pautas que han de tenerse en cuenta para que la normativa de protección de datos puedan aplicarse a los ficheros manuales.

[459] SAN 16 de febrero de 2006, FJ 2. Informe jurídico AEPD, 0453/2008, en el que se entiende que el hecho de que un abogado incorpore a una carpeta en la que cada cliente tiene su apartado constituye un fichero. Informes jurídicos AEPD 0549/2008 y 0078/2009.

[460] Resolución de la APDCM, "La Policía Municipal de un municipio no contravino la normativa de protección de datos a la hora de solicitar a los viandantes de una zona su identificación", en la que se niega la calidad de fichero a carpetas de las Fuerzas y Cuerpos de Seguridad clasificadas por días, meses y años. Resolución de la APDCM, "El archivo de las historias clínicas de los pacientes de un centro joven de un ayuntamiento de la Comunidad de Madrid en el que se dispensa la píldora del día después", en la que se niega la cualidad de fichero a carpetas en las que se contienen datos sanitarios, pero que se organizan en base a códigos correspondientes al número de visitas, en vez de a criterios relacionados con las personas titulares.

[461] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p, 88; GONZÁLEZ MORENO, "La Ley Orgánica de Protección….", cit., 2010, p. 608.

[462] PÉREZ-MADRID, "La autonomía de las confesiones…", cit., 2010, p. 597 y siguientes, expone los argumentos empleados en relación a esta cuestión.

[463] Informe jurídico AEPD, 0378/2008. Resolución de la AEPD, archivo de actuaciones nº E/00254/2008, 24 de noviembre de 2008.

[464] SAN 10 de octubre de 2007, FJ 5: "Los Libros de Bautismo (…) en la medida en que recogen datos de carácter personal (…) con arreglo a criterios preestablecidos que permiten su tratamiento, tienen la consideración de ficheros".

de fichero, a efectos de aplicar la Ley, a los libros bautismales. Sin embargo, en última instancia el TS les negó esta condición por tratarse de documentos que estaban ordenados simplemente atendiendo al criterio de la fecha de bautismo y no a criterios personales[465].

Esta interpretación realizada por los tribunales merece una consideración, independientemente de que se interprete que la cancelación de datos pretendida sobre los ficheros bautismales deba regularse en atención a la LOPD o al Derecho canónico[466]. Por un lado, puede ser objeto de una valoración positiva por cuanto que es lo suficientemente clara como para no generar inseguridad jurídica o confusión. Por otro, desde un punto de vista sustancial, puede ser criticada en la medida en que aboca a una situación de desprotección a los titulares de datos contenidos en ficheros no automatizados. Si el reconocimiento del derecho a la autodeterminación informativa se extiende en la actualidad a los sujetos afectados por tratamientos manuales es porque se es consciente del riesgo que este tipo de operaciones pueden llegar a generar. Si bien es cierto que este riesgo aumenta cuando el criterio según el cual se organiza el fichero hace referencia a las personas titulares de los datos, no lo es menos que, como en el caso de los libros bautismales, dicho riesgo no desaparece porque el criterio de estructuración sea otro. Piénsese en el caso en que estos libros, que recogen datos sobre la orientación religiosa de las personas, se pierden o son sustraídos. Evidentemente, la inaplicación de la normativa de protección de datos a este tipo de ficheros, sobre todo de las medidas de seguridad, favorece que estos riesgos se hagan realidad. Es cierto que en estas situaciones podrían aplicarse normas dirigidas a proteger la intimidad de las personas; sin embargo, resultarían inaplicables las facultades que componen el derecho a la autodeterminación informativa[467].

No se está diciendo aquí que todo tratamiento manual de datos deba quedar sometido a esta normativa, pues este criterio podía llevar a situaciones absurdas, como bien ha apuntado la jurisprudencia[468]. No obstante, el criterio que recoge la Directiva y que tiene aplicación en el ámbito interno puede derivar en la asunción de unos parámetros tan cerrados, que dejen fuera del ámbito de aplicación supuestos de tratamientos que afectan a la autodeterminación informativa, sin que los sujetos afectados puedan ejercer los derechos reconocidos en la LOPD.

En el sector sanitario esta polémica no parece tener gran repercusión. Hay que tener en cuenta que salvo contadas ocasiones toda manipulación de datos que se lleva a cabo se refiere a

[465] STS 19 de septiembre de 2008, FJ 4, argumenta que los libros bautismales no son ficheros, al tratarse de "una pura acumulación de estos (datos) que comporta una difícil búsqueda, acceso e identificación en cuanto no están ordenados ni alfabéticamente, ni por fecha de nacimiento, sino sólo por las fechas de bautismo".

[466] PÉREZ-MADRID, "La autonomía de las confesiones…", cit., 2010, pp. 602-605; GONZÁLEZ MORENO, "La Ley Orgánica de Protección….", cit., 2010, p. 620, apuntan que la apostasía constituye una figura de Derecho canónico, sobre la que las agencias de protección de datos no tendrían capacidad de control, al incardinarse los ficheros bautismales en el marco de la actividad puramente religiosa, protegida por la autonomía de los entes religiosos.

[467] SAN 9 de julio de 2009, FJ 2, en que no se considera aplicable la LOPD a un caso en que una empresa despide a un trabajador por conocimiento de datos de salud, por el hecho de que dicho dato no estuviera incorporado en fichero alguno. MESSÍA DE LA CERDA BALLESTEROS, "El Derecho a la Protección…", cit., 2007, pp. 230-231, no tiene duda alguna sobre la consideración de fichero a efectos de aplicar la LOPD de los ficheros bautismales; ARENAS RAMIRO, "La Sentencia del Tribunal Supremo…", cit., 2008, p. 208, en el mismo sentido.

[468] SAN 22 de abril de 2009, FJ 4, señala en este sentido que la captura de imágenes no es subsumible en el ámbito de aplicación de la LOPD, por cuanto que la grabación no se incorpora a fichero alguno. En todo caso, dicha grabación podría constituir una violación de la intimidad, de acuerdo al artículo 18.1 CE.

información que se encuentra o tiene como destino un fichero. La gran mayoría de veces, además, estos ficheros se ordenan en base a criterios personales, como puede ser el nombre o el número de historia clínica vinculado a cada persona.

IV. BREVE CONSIDERACIÓN SOBRE LO QUE SE ENTIENDE POR TRATAMIENTO.

Se considera necesario en este momento determinar lo que ha de entenderse por tratamiento. Este ejercicio viene motivado, en primer lugar, por la conveniencia de dar un contenido determinado a dicho concepto y, en segundo, por el hecho de que el uso que se hace en la Ley del mismo puede llevar a equívocos.

IV.1. Interpretación del concepto tratamiento en sentido amplio.

La necesidad de dar un contenido concreto al concepto de tratamiento viene determinada por el hecho de que el régimen de protección de datos reconocido en las leyes se aplica a los datos que son susceptibles de tratamiento[469]. Por lo tanto, las operaciones que queden fuera de dicho concepto no se sujetarán a ese régimen jurídico.

En relación al ámbito sanitario se ha afirmado que las funciones que se llevan a cabo necesitan de la manipulación de los datos de carácter personal. La gestión de los datos es una actividad esencial aquí. Desde que se recogen hasta que se suprimen son numerosas las operaciones que se realizan y los usos que se da a los datos de carácter personal, presentando cada uso sus particularidades y propios problemas. La obtención, el almacenamiento, el *outsourcing*, la cesión, la transmisión internacional, la realización de estadísticas, el cruce de datos, etc., son operaciones que se llevan a cabo con normalidad.

La LOPD ha englobado todas estas operaciones en un concepto: el tratamiento. Antes de la entrada en vigor de la Ley, el Convenio de 1981 del Consejo de Europa entendía por tratamiento las operaciones que, siendo en parte o en su totalidad automatizadas, conllevaran el registro de datos, la aplicación a estos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión[470]. La LOPD, siguiendo el criterio marcado por la Directiva europea[471] y la LORTAD[472], define dicho concepto como "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación,*

[469] Artículo 2.1 LOPD.
[470] Artículo 2.c) Convenio 108/1981 del Consejo de Europa.
[471] Artículo 2.b) Directiva 95/46/CE: "*Cualquier operación o conjunto de operaciones efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción*". En este sentido, hay que hacer notar que el Convenio 108/1981 del Consejo de Europa, en su artículo 2.c), a la hora de definir el tratamiento, no englobaba la recogida de datos. Tampoco lo hacía en un inicio la Directiva actual, debido al mimetismo que la primera propuesta de la Directiva acusaba con respecto a la ley alemana que en su artículo 3º definía por separado el tratamiento y la recogida, lo cual suponía la exclusión de esta última operación del ámbito de aplicación de la norma. Es en el texto de 1992 cuando se modifica la definición del concepto tratamiento y se incluye la recogida. Al respecto ver HEREDERO HIGUERAS, *La Directiva...,* cit., 1997, p. 75.
[472] Artículo 3.c) LORTAD: "*Tratamiento de datos: Operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, asó como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*".

bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"[473]. En el mismo sentido se ha expresado el reglamento que desarrolla la Ley[474]. Hoy día está comúnmente asumido que para entender que se está ante un tratamiento no es necesario que la manipulación a llevar a cabo tenga que ser automatizada. De todas formas, ya se ha visto que a la hora de aplicar la Ley a los usos manuales de datos será necesario que dichas operaciones se hagan sobre datos contenidos o destinados a un fichero, que además deberá estar estructurado de una determinada manera[475].

Las normas han apostado por llevar a cabo una definición basándose en un sistema casuístico. Se recoge en los textos normativos un listado de las operaciones que se considera constituyen tratamiento. El amplio listado que se prevé abarca cualquier tipo de operación que pueda llevarse a cabo sobre los datos de carácter personal. En todo caso tampoco parece que este listado sea cerrado, pues la referencia que se realiza en las definiciones a "*cualquier operación*" deja las puertas abiertas a que usos que en principio no estén recogidos en dicha lista puedan quedar amparados por su consideración como tratamiento. En la misma línea parece apuntar el hecho de que en la redacción de la Directiva europea la lista de operaciones que constituyen un tratamiento se configure como un mero ejemplo de las acciones que pueden considerarse como tal: *"cualquier operación (…) como la recogida, el registro (...)*". El empleo del término "como" deja entrever que se trata de un listado a título de ejemplo.

No hay duda de que la definición aportada por la LOPD intenta abrazar todos los usos que puedan darse a los datos de carácter personal[476]. En algún caso ha surgido la duda sobre la consideración como tratamiento de alguna actuación determinada. Concretamente, y al hilo de lo que se dirá a la hora de distinguir los conceptos de dato e información, se ha planteado si el mero conocimiento o la mera visualización de unos datos puede constituir un tratamiento. En caso de respuesta afirmativa la operación será objeto de protección de la LOPD, no así, si se entiende que la respuesta es negativa. En este sentido, un informe jurídico de la AEPD ha aclarado, acertadamente, que la simple visualización constituye un tratamiento de datos[477]. Argumenta esta institución que la definición amplia recogida en las normas justifica la inclusión de esa operación en dicho concepto. Las manipulaciones que permitan el acceso a datos constituyen un tratamiento[478]. Se entiende que, más allá de dicho argumento, la integración de la mera visualización de los datos en el concepto de tratamiento responde a la necesidad de que el derecho a la autodeterminación informativa y la intimidad desplieguen sus efectos desde el momento en que un tercero tenga acceso a la información. Lo contrario haría posible que toda

[473] Artículo 3.c) LOPD.
[474] Artículo 5.1.t) RDLOPD: "*Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no, automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias*".
[475] SAN 12 enero 2007 FJ. 3.
[476] Como se subraya en uno de los informes jurídicos complementarios a la exposición realizada por el Consejero de Sanidad durante su comparecencia ante la comisión de sanidad del parlamento vasco el 23 de mayo de 2002 a fin de dar cuenta del proceso de centralización de los datos de los pacientes recogidos en los centros de salud de Osakidetza, "no existe apenas limitación teórica en cuanto al tipo de actividades que pueden entenderse incluidas en el concepto de tratamiento".
[477] Informe jurídico AEPD, 0179/2009.
[478] Resolución de la AEPD, R/02773/2009, 15 de enero de 2010. Procedimiento AP/00057/2009.

visualización fuera legítima, lo que dejaría desnudas a las personas ante la curiosidad de terceros. La mera visualización de los datos de carácter personal deberá encontrar, por lo tanto, justificación en las normas. En este sentido, el mero acceso por parte de un ciudadano a, por ejemplo, un Registro en el que aparezcan datos de carácter personal puede considerarse un tratamiento[479]. De la misma forma, la puesta a disposición del público en una página web de datos de carácter personal constituye un tratamiento de datos[480].

La necesidad de que la definición tenga ese carácter amplio esta justificada. Es cierto que no todas las operaciones pueden llegar a constituir la misma amenaza para el derecho a la autodeterminación informativa. No es lo mismo la cancelación de unos datos, que realizar una transferencia internacional a un país que no guarda un nivel de protección de datos adecuado. Sin embargo, es innegable que todas estas operaciones afectan al derecho que los ciudadanos tienen sobre la información que les concierne en mayor o menor medida. La amplia definición dada en las normas trata de otorgar al titular de los datos la máxima protección posible, aplicando el régimen jurídico contenido en su articulado a todo tipo de operaciones que se puedan llevar a cabo sobre los datos de carácter personal.

IV.2. Breve referencia a los problemas de interpretación que derivan del articulado de la LOPD con el uso del concepto tratamiento.

La definición dada del concepto de tratamiento no plantea, en principio, problemas de comprensión. Como ya se ha dicho, el sentido amplio que se otorga al concepto parece querer abarcar todas las operaciones que se puedan realizar sobre los datos de carácter personal. Los problemas comienzan cuando del articulado de la Ley deja entreverse, que en determinados preceptos el concepto de tratamiento guarda un sentido diferente al genérico citado.

En algunas ocasiones la LOPD utiliza dicho término de forma restrictiva, entendiéndolo como otra operación más de las expresadas en la definición genérica dada, es decir, como una fase más en el uso de los datos, igual que la recogida o la cesión, y no como el concepto expansivo que engloba a todas las operaciones. Esta idea se deduce, por ejemplo, del artículo 7.3 relativo al tratamiento de datos de salud, al disponer que estos datos, entre otros, podrán ser “recabados, tratados y cedidos” en determinadas condiciones. Necesariamente, al emplear dichos términos de forma separada parece que han de tener un sentido propio, de manera que el tratamiento no sería otra cosa que un uso más, al igual que la recogida o la cesión[481]. Ambas acepciones del concepto tratamiento, la amplia y la restrictiva, son correctas, pues técnicamente el tratamiento es toda operación que se realice sobre unos datos de carácter personal, pero también una fase más, junto a la recogida o la cesión, dentro de ese proceso más amplio al que se somete a dichos datos.

El problema del uso del concepto de tratamiento con diferentes sentidos viene por el hecho de que el legislador no aclara en la norma cuándo se utiliza en sentido amplio o restrictivo. La

[479] Informe jurídico AEPD, 96/2008. En el que se considera tratamiento el acceso de un ciudadano a documentos obrantes en un Ayuntamiento en el que aparecen datos de carácter personal.
[480] Resolución de la AEPD R/02350/2009, 28 de octubre de 2009. Procedimiento AP/00039/2009.
[481] Pueden verse en el mismo sentido los artículos 44.3.c) y 4.1 LOPD. De su contenido parece deducirse, también, que el tratamiento es, simplemente, una fase más, al igual que la recogida o la cesión.

determinación de lo que se entiende por tratamiento es verdaderamente importante, y no sólo porque este concepto constituye una de las instituciones centrales de la LOPD[482]. Cuando la Ley regula en su articulado diferentes operaciones: recogida, tratamiento, cesión, etc., lo hace exigiéndose unos requisitos concretos para que las mismas puedan llevarse a cabo: necesidad de consentimiento, obligación de informar, entre otros. Cuando en dichas disposiciones se hace referencia al tratamiento habrá que aclarar si se hace en un sentido amplio o no, para concretar si los requisitos exigidos en el artículo para poder llevarlo a cabo se aplican a unas operaciones o a otras. En este sentido, la redacción de la Ley deja mucho que desear, pues al emplear el concepto en sentido amplio o restrictivo de manera aleatoria puede llegar a crear situaciones de confusión e inseguridad jurídica[483].

Los problemas interpretativos que derivan del uso indistinto de la acepción amplia o restrictiva se plantean en preceptos concretos en que aparece solo o acompañado por otros, como el de recogida y cesión. Por ejemplo, cuando la LOPD entra a regular los ficheros policiales, señala que las Fuerzas y Cuerpos de Seguridad pueden recoger y tratar los datos relativos a la salud de las personas, entre otros, para la realización de investigaciones concretas[484]. La no inclusión en este precepto del concepto de cesión lleva a tener que plantearse si esta regulación se aplica a esta operación o no. En principio parece que si el legislador trata de otorgar un régimen jurídico específico a este tipo de ficheros, esta regulación deberá ser aplicada a todas las operaciones llevadas a cabo en este ámbito. De esta forma, cabría entender el concepto de tratamiento en un sentido relativamente amplio que incluyera la operación de cesión. Esta cuestión será analizada más adelante, pero sirve ahora para poner de manifiesto los problemas de interpretación que puede llegar a generar la redacción de la Ley.

En lo que respecta al tratamiento de los datos de salud diferentes preceptos plantean problemas parecidos al citado. Muchos de ellos serán resueltos a lo largo de este trabajo, sin embargo, merece la pena aclarar en este momento el contenido de los principales artículos que regulan la manipulación de este tipo de información. El artículo 7.3 LOPD señala que, entre otros, los datos de salud sólo podrán recabarse, tratarse o cederse cuando, por razones de interés general, así lo disponga una ley o el afectado otorgue su consentimiento expreso. Se distinguen aquí la recogida, el tratamiento y la cesión. El artículo 7.6 dispone que podrán tratarse, entre otros, los datos de salud, se entiende que sin el consentimiento del titular, cuando la finalidad sea la prevención o el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que el tratamiento se realice por un profesional u otra persona sujeta a la obligación de secreto. En este precepto sólo se habla del tratamiento. Por su parte, el artículo 8 dispone que, sin perjuicio de lo que establece el artículo 11

[482] HEREDERO HIGUERAS, *La Ley*..., cit., 1996, p. 74: "El concepto de tratamiento es clave para el acotamiento del ámbito de aplicación de la ley".
[483] SAN 7 de noviembre de 2002 FJ 2, en la que se plantea el problema de que a la hora de aplicar una sanción recogida en el artículo 44.3.c) de la LOPD, dicho artículo queda solapado por el que le sigue, 44.3.d), pues, resumiendo, si en el primero se castiga la recogida no acorde con los principios de la LOPD y en el segundo el tratamiento, en general, de los datos no acorde con los citados principios, y teniendo en cuenta que en el artículo 3º de la LOPD se considera que la recogida queda englobada por el más amplio concepto de tratamiento, el artículo 44.3.c) deja de tener sentido pues el tipo que recoge ya queda sancionado en el artículo posterior.
[484] Artículo 22.3 LOPD.

respecto de la cesión, los datos de salud podrán ser tratados por los profesionales sanitarios en los centros sanitarios públicos y privados de acuerdo a la legislación sobre sanidad. Se distinguen aquí el tratamiento y la cesión.

Como se puede ver, en estas disposiciones se emplean indistintamente los conceptos de tratamiento, recogida y cesión. Se plantea, por lo tanto, la duda de a qué operaciones en concreto se aplica el régimen jurídico recogido en dichos preceptos. Este problema no se da, por ejemplo, en la Directiva europea, donde el legislador europeo continuamente hace referencia al "tratamiento", entendido en un sentido amplio, y no a otros términos, evitando así posibles confusiones. Tiene sentido la fórmula empleada por esta norma por cuanto lo normal será, más allá de supuestos puntuales, que toda operación que se lleve a cabo sobre un tipo de dato determinado, como los de salud, en un contexto concreto, deba sujetarse a unas mismas reglas mínimas de protección[485].

En relación a estos preceptos los problemas de interpretación pueden darse sobre dos puntos. En primer lugar, en relación a la confusión que genera el uso del término tratamiento, junto a los de recogida y cesión, en sentido más o menos amplio. Este hecho plantea dudas a la hora de determinar el régimen jurídico que deba aplicarse a cada una de las fases: si es necesario el consentimiento del titular para alguna de las fases, para unas sí y para otras no, etc. En segundo lugar, aunque relacionado con el punto anterior, el uso indistinto del término tratamiento en sentido amplio o estricto plantea la duda de si, cuando en los preceptos de la Ley se limitan las facultades que componen el derecho a la autodeterminación informativa, fundamentalmente el consentimiento, estos límites se aplican a todas las fases o sólo a unas. Estos problemas de interpretación han de analizarse en cada una de las disposiciones citadas.

La primera de las disposiciones comentadas señala que la recogida, tratamiento y cesión de los datos de salud requerirán, salvo ley en contrario, del consentimiento del titular de los datos. Parece que el tratamiento, en este caso, se refiere a una operación concreta, diferente a la recogida y a la cesión, que nada tiene que ver con la definición amplia anteriormente citada. Partiendo de una interpretación literal del precepto se puede concluir que el artículo requiere el consentimiento individualizado, tanto para la recogida como para el tratamiento y la cesión. Esta lectura podría incluso tener respaldo en el artículo 44.3.c) de la Ley, que tipifica como infracción grave la recogida de datos de carácter personal sin recabar el consentimiento expreso del titular de los datos, cuando éste sea exigible. A partir de esta consideración, la conclusión a sacar sería sencilla: habría que pedir el consentimiento primero para la recogida, luego para el tratamiento, y, por fin, para la cesión[486].

El requerimiento del consentimiento para la cesión de datos está plenamente justificado debido al evidente riesgo que plantea dicha operación, pues supone sacar unos determinados

[485] Artículo 8 Directiva 95/46/CE, que regula la manipulación de datos de salud, se refiere en todo momento al concepto de "tratamiento", sin emplear los de recogida o cesión.
[486] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 281, parece guiarse en este sentido.

datos de carácter personal del ámbito en el que estaban siendo manipulados[487]. La cesión conlleva un nuevo tratamiento que ha de ser, de inicio, autorizado por el titular de los datos. No ocurre lo mismo con la recogida, en la que requerir un consentimiento individualizado se entiende que carece de sentido alguno. Tener que solicitar el consentimiento del titular para la recogida de los datos, para que después haya que exigir, otra vez, dicho consentimiento para su tratamiento (entendido en sentido estricto) carece de justificación, pues supondría burocratizar en exceso la tarea del tratamiento de datos. Parece lógico pensar que si se está consintiendo el tratamiento se estará autorizando también la recogida, y viceversa. El único supuesto en que la recogida y el posterior tratamiento pueden requerir de consentimientos diferentes se limita al caso en que, una vez consentida la recogida y el posterior tratamiento de unos datos, el responsable del fichero quiera llevar a cabo un nuevo tratamiento, distinto al que motivó la recogida inicial.

El segundo de los preceptos es el que plantea menores problemas. El uso, únicamente, del concepto tratamiento da a entender que en el artículo 7.6 se emplea dicho término en sentido amplio, incluyendo todo tipo de operación que se vaya a realizar con estos datos. Esta redacción trae causa de lo dispuesto a este respecto por la Directiva europea. Podría decirse que las finalidades que se recogen en dicho precepto justifican un régimen jurídico que afecta a todo tratamiento de los datos sensibles. Es decir, en este precepto se prevé un régimen jurídico común para todo tipo de operaciones que se quieran llevar a cabo con dicha información, siempre y cuando los objetivos que se persigan sean los previstos en la disposición.

El tercero de los preceptos citados se refiere a la cesión y al tratamiento. La cesión se regulará, en principio, de acuerdo a lo dispuesto en el artículo 11 de la Ley y el tratamiento en base a la legislación sanitaria. Nada se dice sobre la recogida. El principal problema se plantea, por lo tanto, con la inclusión o no de la fase de recogida de datos de carácter personal en el concepto de tratamiento, y en la determinación de la necesidad o no de exigir el consentimiento al titular de los datos en esta primera fase de obtención de los datos. ¿Se puede entender que en este precepto la recogida y el tratamiento son operaciones diferenciadas que exigen un consentimiento individualizado? Es decir, ¿puede plantearse que por un lado la recogida exija su consentimiento, y por otro, el tratamiento el suyo?[488] Como luego se verá, más allá de lo dispuesto para la cesión, de la remisión a la legislación sanitaria parece desprenderse la idea de que en el ámbito sanitario los datos de salud pueden ser manipulados en muchos casos sin el consentimiento del titular. De esta forma, dependiendo de si el concepto de tratamiento se interpreta en esta disposición de forma amplia o restrictiva, se podrá entender que el consentimiento se exceptúa para la recogida y el tratamiento en sentido estricto, o sólo para este último. Si el concepto tratamiento se interpreta en sentido restrictivo, la fase de la recogida

[487] SAN 29 de noviembre de 2002, FJ 3, en relación a un supuesto en que una empresa sufre una escisión y los datos obrantes en la misma se reparten entre las distintas empresas nuevas creadas a raíz de dicha escisión. En relación a la cesión de datos que se produce, el Tribunal subraya los riesgos específicos que generan dichas transmisiones.

[488] SOUVIRÓN, "En torno a la Juridificación...", cit., 1994, p. 152, señala que el "tenor del precepto (en referencia al artículo 6.1 de la LORTAD que disponía que "*el tratamiento automatizado de los datos de carácter personal requerirá con carácter general el consentimiento del afectado salvo que la ley disponga otra cosa")* resulta ciertamente abstracto, sin que el mismo delimite claramente si ese consentimiento va a ser preciso además de para el "tratamiento" también para la recogida y cesión de los datos (como expresa y minuciosamente señala el artículo 7 para los datos "sensibles" en él contemplados)".

quedaría fuera del campo de aplicación de dicho precepto, aplicándosele, a falta de otra disposición, el artículo 7.3 que regula el tratamiento de datos relativos a la salud y que exige el consentimiento para llevar a cabo la recogida de dichos datos.

Algunos autores han visto en este precepto una excepción al consentimiento para el tratamiento de los datos pero no para la recogida. De esta forma el consentimiento sería en todo caso exigible por el paciente en la fase de la recogida, aún cuando para el tratamiento de los datos no hiciera falta dicho requisito[489]. Esta interpretación carece de un fundamento sólido. Si se considera que el tratamiento de los datos relativos a la salud sin el consentimiento del titular de los datos está justificado atendiendo a bienes jurídicos que merecen mayor protección, no se puede entender que la mera recogida de los mismos datos requiera el citado consentimiento, pues la recogida es requisito imprescindible para el posterior tratamiento. Sin recogida no hay tratamiento. Si se entiende que este tratamiento es necesario para la salvaguarda de un interés particular o colectivo superior al derecho a otorgar el consentimiento, es coherente entender que la recogida, al igual que el tratamiento, no necesitará del consentimiento del titular[490].

Que la recogida pueda realizarse sin necesidad de recabar el consentimiento del titular puede plantear problemas prácticos. En el ámbito tributario los ciudadanos están obligados a aportar la información necesaria para que la Administración tributaria pueda practicar la liquidación de los tributos pertinentes[491]. Evidentemente, en el ámbito sanitario los pacientes no se encuentran obligados a remitir la información que no quieran sobre su estado de salud, no, por lo menos, cuando lo que está en juego es únicamente su salud. Se requiere que el titular de los datos otorgue voluntariamente la información. Bien sea vía oral en una consulta o a través de intervenciones consentidas de carácter médico, salvo excepción, el individuo ha de prestar la información requerida de manera voluntaria, para que sea tratada posteriormente con fines principalmente sanitarios. En este sentido, la jurisprudencia, cuando se ha referido a los problemas que plantea la recogida de información a través de intervenciones corporales, ha

[489] VIZCAÍNO CALDERÓN, *Comentarios a la Ley…,* cit., 2001, p. 137; FERNÁNDEZ SALMERÓN, *La Protección...*, cit., 2003, p. 276 cita a VIZCAÍNO CALDERÓN quien entiende que en el artículo 8º de la LOPD no se exceptúa del consentimiento la operación de recogida de datos de carácter personal, independientemente de que el tratamiento sí quede exceptuado de dicho consentimiento.

[490] FERNÁNDEZ SALMERÓN, *La Protección...*, cit., 2003, p. 276, entiende que la solución a la que llegan autores como VIZCAÍNO CALDERÓN no es razonable, pues "si el suministro de los datos relativos a la salud es una carga para el afectado, parece evidente que éste consiente implícitamente dicha recogida cuando los proporciona, de modo que huelga cualquier referencia a la mediación o no del consentimiento". Considera este autor que "a pesar de que el artículo 7.3 LOPDP se refiera al consentimiento expreso en la recogida de estos datos (...) no cabe hablar de una declaración de voluntad tal en relación con esta operación (...). Las que pueden ser objeto de consentimiento expreso son propiamente las operaciones ulteriores de utilización de los datos".

[491] Artículo 93.1 Ley 58/2003, 17 de diciembre de 2003, General Tributaria: "*Las personas físicas o jurídicas, públicas o privadas, así como las entidades mencionadas en el apartado 4 del artículo 35 de esta Ley, estarán obligadas a proporcionar a la Administración tributaria toda clase de datos, informes, antecedentes y justificantes con trascendencia tributaria relacionados con el cumplimiento de sus propias obligaciones tributarias o deducidos de sus relaciones económicas, profesionales o financieras con otras personas*". Artículo 192.1 Ley 58/2003, 17 de diciembre, General Tributaria: "*Constituye infracción tributaria incumplir la obligación de presentar de forma completa y correcta las declaraciones o documentos necesarios, incluidos los relacionados con las obligaciones aduaneras, para que la Administrasción tributaria pueda practicar la adecuada liquidación de aquellos tributos que no se exigen por el procedimiento de autoliquidación, salvo que se regularice con arreglo al artículo 27 de esta Ley*". GUICHOT, *Datos Personales…,* cit., 2005, p. 418. STS 26 de noviembre de 2008, FFJJ 3 y 4, en la que se impone la obligación de aportar la información requerida a la Administración Tributaria.

considerado que la necesidad de que sea el paciente quien autorice dichas operaciones se fundamenta no sólo en el principio de autonomía sino también en la protección de la integridad moral y física del paciente[492]. Obligar a las personas a dar información sobre su salud podría llegar a justificar intervenciones corporales forzosas. Esta situación atentaría contra diferentes derechos fundamentales.

Esto no quiere decir, sin embargo, que sea necesario el consentimiento del titular para llevar a cabo la recogida de los datos de salud en el ámbito sanitario. La falta de obligación de remitir la información de carácter personal se produce en este ámbito porque, como se verá más adelante, entran en juego diferentes bienes jurídicos que hacen imposible justificar esa obligación. Sin embargo, desde el punto de vista de la autodeterminación informativa, dejando a un lado otros derechos que podrían quedar afectados en operaciones como las intervenciones corporales forzosas, parece admisible que la recogida se pueda llevar a cabo sin la necesidad del consentimiento del titular. Por ejemplo, puede plantearse si para proteger la salud de una persona se puede recabar información sobre la misma a partir de un tercero. Se entiende aquí que la recogida de estos datos, por ejemplo cuando se trata de enfermedades mentales, sin el consentimiento del titular está plenamente justificada.

En términos generales es cierto que la recogida y el posterior tratamiento son fases diferentes que plantean problemáticas diferentes, pero realizar de partida la interpretación que se ha expuesto del artículo 8 de la Ley carece de sentido práctico. Desde el punto de vista del derecho a la autodeterminación informativa parece difícil que se pueda encontrar un supuesto en que no se permita el tratamiento sin consentimiento y se permita la recogida, o al revés.

De lo dicho se pueden extraer algunas conclusiones. La distinción de las distintas fases por las que puede pasar la manipulación de unos datos se antoja acertada, por cuanto que cada una de ellas presenta unos problemas particulares y exige unos requisitos específicos para que puedan ser llevadas a cabo[493]. Es evidente que la cesión necesita, en principio, del consentimiento; que la transferencia internacional exige de un mayor control por las instituciones; y que la recogida es el momento ideal para llevar a cabo determinadas acciones como la información al titular de los datos. Sin embargo, la genérica definición que se realiza en la LOPD del concepto de tratamiento plantea problemas de interpretación al emplearse después este mismo concepto de manera distinta al fijado en la definición. La interpretación adecuada de este concepto deberá realizarse en cada caso, atendiendo a si en el precepto en cuestión se recogen otras operaciones o no. Lo importante es subrayar el reconocimiento de distintas operaciones en la manipulación de los datos y ser conscientes de que cada uso exige sus propias garantías debido a los problemas particulares que plantean para los derechos fundamentales. Así, cuando la LOPD utiliza el término tratamiento, habrá que atender a las circunstancias concretas o el contexto determinado en el que se emplea dicho término, para poder fijar los requisitos necesarios para llevar a cabo los usos correspondientes.

[492] STC 24 de septiembre 2007, FJ. 3.
[493] VIZCAÍNO CALDERÓN, *Comentarios a la Ley...*, cit., 2001, p. 78.

V. EL DATO DE CARÁCTER PERSONAL SANITARIO.

La delimitación del concepto dato de carácter personal sanitario es una tarea que hay que llevar a cabo en este momento. Esta delimitación se realiza con fines estrictamente jurídicos, teniendo en cuenta que de distintas interpretaciones de estos términos pueden derivarse consecuencias muy diferentes.

La aprobación en los últimos años de normas tan relevantes como la Ley Orgánica 10/2007, de 8 de octubre, reguladora de la Base de Datos Policial sobre Identificadores obtenidos a partir de ADN, la Ley 14/2007, de 3 de julio, de Investigación Biomédica y el RDLOPD ha puesto nuevamente sobre la mesa un debate que no deja de estar abierto a pesar de referirse a una cuestión sobre la que se ha escrito en numerosas ocasiones. Se trata de la necesidad de dar una definición y contenido determinado al concepto de "dato de carácter sanitario".

Para llevar a cabo ese ejercicio será necesario el estudio de otros conceptos, y es que el "dato sanitario" es en primer lugar "dato de carácter personal", en segundo lugar "dato relativo a la salud" y por último lo que se ha denominado "dato sensible". De lo que se entienda por estas expresiones dependerá el contenido del concepto "dato sanitario". Se tratará de aportar una serie de reflexiones en torno a estos conceptos.

V.1.El dato de carácter personal.

V.1.1. Introducción.

El dato sanitario es antes de nada dato de carácter personal, por lo que resulta imprescindible realizar una aproximación al significado de esta expresión.

En principio, la totalidad de las normas coinciden a la hora de definir el dato de carácter personal. Desde la Unión Europea[494], el Consejo de Europa[495], el Estado[496] y las distintas Comunidades Autónomas[497] que han regulado, en lo que les corresponde, la protección del derecho a la autodeterminación informativa, se ha entendido que es dato de carácter personal "cualquier información relativa a una persona física identificada o identificable".

De una primera lectura de dicha definición se podría concluir que se trata de una delimitación acertada, ya que fija el contorno de la realidad "dato de carácter personal" de forma en principio reconocible. Puede deducirse de la misma que para considerar la existencia de un dato de carácter personal hay que contar con la información y con la identidad de la persona a la que se

[494] Artículo 2.a) Directiva 95/46/CE; Artículo 2.a) Reglamento Nº 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la Protección de las Personas Físicas en lo que respecta a Tratamiento de Datos Personales por las Instituciones y los Organismos Comunitarios y a la Libre Circulación de estos Datos, en Diario Oficial de las Comunidades Europeas L. 8, 12 de enero de 2001.
[495] Artículo 2.a) Convenio 108/1981 del Consejo de Europa.
[496] Artículo 3.a) LOPD.
[497] Artículo 3.a) Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid y artículo 3.a) Ley 2/2004 de 25 de febrero de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

refiere dicha información[498]. Sin embargo, en la práctica, a la hora de identificar esos datos de carácter personal en los supuestos concretos, surgen los problemas debido a la indeterminación de varios de los términos empleados en la definición.

Se puede observar que las normas han optado por dar una definición general del concepto. Frente a esta fórmula tenían la posibilidad de hacer la delimitación a través de un sistema casuístico, pero esta segunda opción plantearía graves problemas de seguridad jurídica. La adopción del sistema casuístico conllevaría que la norma tuviera que hacerse eco de una lista de todos los datos que tienen la consideración de información de carácter personal a efectos de aplicar la normativa de protección de datos[499]. Este sistema acarrearía un riesgo de envergadura: el peligro de que el legislador dejara fuera supuestos concretos que sí son información de carácter personal o formatos que pudieran aparecer en un futuro y que no se recogieran en la Ley. La inseguridad jurídica que resultaría de una tal definición hace que se valore de manera positiva la adopción en las normas de la fórmula genérica a la hora de definir el concepto[500]. Esta fórmula, sin embargo, conlleva también sus riesgos. Es posible que la definición se plantee en términos excesivamente genéricos y no sea identificable después en la práctica.

En la definición que se ha dado por las normas arriba citadas, si bien es de apreciar el esfuerzo del legislador por dar un contenido al concepto de dato de carácter personal, hay que criticar la ambigüedad con la que ha quedado fijado. Es evidente que se trata de una definición excepcionalmente amplia[501]. A pesar de que cierta amplitud en la misma puede ser positiva en cuanto posibilita su adecuación a nuevas circunstancias y que nuevas realidades puedan ser incluidas en dicha definición (más aún en el caso de las Nuevas Tecnologías en el que el avance es rápido y constante)[502], la indeterminación resulta un verdadero problema en la práctica si no se establecen criterios mínimamente estrictos y claros que posibiliten la identificación del concepto en los casos particulares. Así, por ejemplo, en el caso estatal, ha tenido que ser la AEPD la que en muchos supuestos ha ido determinando si se consideran dato de carácter personal una serie de supuestos concretos como, por ejemplo, las direcciones IP[503], el correo electrónico[504] o el número de una finca registral[505].

En las siguientes líneas se tratará de aclarar qué se entiende por "cualquier información relativa a una persona física identificada o identificable". Para realizar un análisis riguroso de

[498] APARICIO SALOM, *Estudio sobre...*, cit., 2000, p. 43, señala "que para que exista un dato de carácter personal es preciso que existan dos elementos, la información y la persona a la que concierne dicha información".
[499] MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 28.
[500] HERRÁN ORTIZ, *La violación...*, cit., 1998, pp. 210-211
[501] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007: "esta definición refleja la intención del legislador europeo de mantener un concepto amplio de <<datos personales>>". GUICHOT, *Datos Personales…,* cit., 2005, p. 209; DEL CASTILLO VÁZQUEZ, *Protección de Datos*…, cit., 2007, p. 329; PIÑAR MAÑAS, "Concepto de dato…", cit., 2010, p. 193.
[502] VIZCAÍNO CALDERÓN, *Comentarios a la Ley...*, cit., 2001, p.72
[503] Informe jurídico AEPD, 327/2003, en el que se reconoce la consideración de estas direcciones como datos de carácter personal, en la medida en que hoy día, para muchos agentes de Internet es realmente factible vincular la dirección IP con la identidad del usuario. PIÑAR MAÑAS, "Concepto de dato…", cit., 2010, p. 206 y siguientes.
[504] Informe jurídico AEPD, "Dirección de correo electrónico", 1999, e Informe jurídico AEPD, 469/2006, en el que se afirma que las direcciones de correo electrónico son datos de carácter personal en la medida en que hagan referencia a su titular.
[505] Informe jurídico AEPD, 0034/2010.

dicha definición lo más acertado es proceder al estudio de los diferentes términos que contiene la misma, así, "cualquier información", e "identificada o identificable".

V.1.2.Sobre la amplitud de la expresión "cualquier información".

Si bien los términos a los que se hace referencia en este momento son de uso cotidiano y no plantean problemas de comprensión de envergadura, se considera que es importante situarlos en el contexto en el que se van a emplear.

A) En primer lugar, se tratará de dar un contenido determinado al término información. Esta aclaración es importante en la medida en que la definición asumida por las normas del concepto "dato de carácter personal" se refiere a la información. La mayoría de las normas emplean indistintamente los términos datos e información. En el caso de la LOPD, por ejemplo, su encabezado se refiere a los datos, mientras que la definición habla de información. Podría parecer que ambos conceptos son sinónimos. Sin embargo, existen diferencias que merecen analizarse para comprender con exactitud el alcance de la definición que se da en las normas al concepto "dato de carácter personal". Esta distinción se realiza con fines simplemente aclaratorios, al objeto de determinar el contenido de la definición, pues en la práctica información y dato se utilizan de forma aleatoria tanto por las normas como por los tribunales.

Las normas, ya se ha dicho, no hacen referencia a esta cuestión. En alguna ocasión, en el ámbito del Consejo de Europa se ha reconocido que hay diferencias entre los conceptos de dato e información, si bien se ha acabado asumiendo que en la práctica ambos términos se emplean como sinónimos[506]. Tampoco la jurisprudencia ha marcado una línea interpretativa que ayude a distinguirlos. Ha de atenderse, por lo tanto, a la doctrina para profundizar en este extremo.

Como punto de partida se ha entendido que es información, la "comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada", y "dato" el "antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho"[507]. Si bien se trata de conceptos íntimamente relacionados entre sí, no se puede afirmar que se identifiquen el uno con el otro.

La doctrina se ha referido a esta cuestión dando criterios que pueden servir para distinguir el dato y la información. Se ha dicho que la información es "el conjunto de noticias, comunicados, informes o datos necesarios para algo o que interesan a alguien"[508], o "que la información es conocimiento, documentación o noticia formalizada o estructurada en función de determinados fines"[509]. En esta línea se ha considerado que "dato (...), o la documentación –entendida como conjunto de datos- son las noticias en su origen, sin haber sido sometidas a ningún tipo de

[506] *Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector* y R*esolution (73)22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector* adoptadas por el Comité de Ministros del Consejo de Europa el 20 de septiembre de 1974, y el 26 de septiembre de 1973, en las que viene a decir el Consejo de Europa que aunque existen pequeñas diferencias entre ambos conceptos, en la resolución serán empleados como sinónimos.
[507] Diccionario de la lengua de la Real Academia Española, http://www.rae.es/.
[508] VELAZQUEZ BAUTISTA, *Protección Jurídica...,* cit., 1993, p.23.
[509] PÉREZ LUÑO, *Nuevas Tecnologías...,* cit., 1987, p.23.

tratamiento ni adecuación. Cuando el dato, o la documentación –como conjunto de datos- son sometidos a un tratamiento o adecuación a un fin, para obtener un resultado elaborado, se convierten en información. La información será", según este autor, "el resultado orientado y adecuado a un fin determinado"[510]. De estas aclaraciones se puede deducir que la información y el dato se refieren a la misma realidad o al mismo objeto, con la diferencia del elemento teleológico: la información es dato empleado con un determinado fin[511]. El dato es previo a la información, y cuando aquel es utilizado, manipulado, tratado con un determinado fin se convierte en información.

Partiendo de lo que se acaba de decir, si se atiende a la definición dada en la Ley sobre el concepto "dato de carácter personal", que se refiere a la información, y haciendo una interpretación literal de su contenido, podría llegarse a la conclusión de que el dato, como base de la que extraer información, quedaría excluido del ámbito de aplicación de la Ley. La LOPD se aplica a la información, por lo que el dato, como tal, quedaría fuera del ámbito de aplicación de la misma. Lo cierto es que en la práctica no es fácil imaginar una base de datos o fichero que no se vaya a emplear con una finalidad determinada, por lo que lo dicho no tiene gran aplicación práctica. Sin embargo, esta aclaración puede servir para plantear una cuestión de relevancia. Cabe preguntarse si por "fin" se puede entender "cualquier fin". ¿Es el conocimiento un fin en sí mismo? ¿Basta con que el fin del tratamiento de los datos sea el conocimiento para que los datos se conviertan en información y pueda ser aplicable la LOPD?

Los ficheros destinados al uso personal o doméstico quedan fuera del ámbito de aplicación de la Ley[512]. Partiendo de esta previsión podría parecer que la respuesta adecuada es la negativa. Cuando en la LOPD se habla del uso personal de los datos, podría entenderse que se hace referencia al hecho de que una persona tenga acceso a dichos datos simplemente para conocerlos. Si se realizara esta interpretación, un fichero que contiene datos con el exclusivo fin de conocerlos no estaría sujeto a la LOPD. El fin, que sería el mero conocimiento de los datos, conllevaría que éstos no pudieran ser considerados como información, por lo que no se aplicaría la Ley. Como bien han señalado la doctrina y la jurisprudencia, cuando la Ley excluye los ficheros de uso personal de la aplicación de la LOPD no lo hace porque el fin de dichos ficheros sea exclusivamente el conocimiento personal de los datos. La exclusión se justificaría por el hecho de que la manipulación de los datos se lleva a cabo en una esfera exclusivamente personal[513], en relación a una actividad equiparable a la que se puede desprender de ese tipo de relaciones[514],

[510] DAVARA RODRÍGUEZ, *La Protección...*, cit., 1998, pp.15-16.
[511] GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 72.
[512] Artículo 2.2 LOPD: "*El régimen de protección de los datos de carácter personal que se establece en la presente Ley orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas*".
[513] STJUE 16 de diciembre de 2008, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy y otros, asunto C-73/07, FJ 44: en relación a la aplicabilidad de la Directiva a los tratamientos exclusivamente personales o domésticos, señala que no se aplica a "actividades que se inscriben en el marco de la vida privada o familiar de los particulares". SAN 15 de junio de 2006, FJ 3, que define la esfera personal como la que afecta a la "esfera más íntima de la persona, a sus relaciones familiares y de amistad y que la finalidad no sea otra que surtir efectos en esos ámbitos". LESMES SERRANO, "Artículo 2…", cit., 2008, p. 79; MEGÍAS QUIRÓS, "Ficheros mantenidos…", cit., 2010, p. 121.
[514] Informe jurídico de la AEPD, 0615/2008, en la que se considera que el intercambio de fotografías en un colegio constituye una actividad encuadrable en ese tipo de relación personal.

independientemente del fin. El argumento citado, por lo tanto, no tiene aplicación para justificar la respuesta negativa a la pregunta planteada.

Se entiende aquí que el hecho de que el fin de un uso de los datos sea el mero conocimiento de los mismos convierte a los datos en información, estando sujeta dicha manipulación a los principios de la LOPD. Parece lógico entender que desde el momento en que una persona conoce el dato éste se convierte en información. Lo mismo se desprende de la definición que da la Real Academia Española del concepto de dato, al considerarlo antecedente para llegar al conocimiento de algo. Este matiz, puede tener una gran importancia en el ámbito de la protección de datos de carácter personal. Cuando la LOPD afirma que protege la información, es decir, el dato empleado con un fin, hay que entender que no hace falta que el dato se utilice, por ejemplo, con el fin de mandar publicidad a diferentes usuarios o para desarrollar una investigación policial. Bastaría con que el fin fuera el conocimiento del dato para que se interprete que se está ante información y que, por lo tanto, entra en el ámbito de aplicación de la LOPD[515]. Hay que tener en cuenta que uno de los bienes jurídicos que trata de proteger la LOPD es la intimidad[516], que se podría definir, en sentido estricto, como el ámbito interno que no se quiere que se conozca por terceros.

B) Fijado ya lo que se puede entender por información, es necesario detenerse en el análisis del calificativo "cualquier". El dato de carácter personal puede ser "cualquier información". La importancia de este calificativo deriva del hecho de que abraza tanto la información que puede resultar más relevante para las personas, caso de la ideología, la vida sexual o los datos sobre la salud, como la información que de inicio pudiera parecer más irrelevante, como una dirección o el correo electrónico.

La derogada LORTAD hablaba de la necesidad de proteger las facetas de la "*personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado*"[517]. El nuevo reglamento que desarrolla la LOPD, por su parte, siguiendo lo que ya establecía la Directiva europea[518], define los datos de carácter personal como *"cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"*[519]. El hecho de que se haga mención a todo tipo de formatos da a entender que se quiere otorgar un sentido

[515] Esta consideración amplia de lo que se ha de considerar por información, a efectos de aplicar la normativa de protección de datos, se deja entrever en el campo de la videovigilancia. La mera captación de imágenes convierte a éstas en información. Es más, incluso se llega a afirmar, a pesar de ser una cuestión polémica, que dicha captación constituye un tratamiento de datos, incluso sin necesidad de que las imágenes queden guardadas o registrados en fichero alguno: SAN 24 de enero 2003, FJ 3. ARZOZ SANTISTEBAN, "Videovigilancia y Derechos…", cit., 2002, p. 151; GOÑI SEÍN, *La Videovigilancia…,* cit., 2007, pp. 94-95; ARZOZ SANTISTEBAN, *Videovigilancia, seguridad…,* cit., 2010, pp. 138-143.

[516] Artículo 1.1 LOPD.

[517] Exposición de Motivos LORTAD. TÉLLEZ AGUILERA, *Nuevas Tecnologías...,* cit., 2001, p.64. Este hecho de que la información, en principio, irrelevante puede convertirse en trascendental al ponerla en relación con otra, se ha denominado la "teoría de los mosaicos", ya que con los datos de carácter personal ocurre lo mismo que "con las pequeñas piedras que forman los mosaicos, que en sí no dicen nada pero unidas pueden formar conjuntos plenos de significado".

[518] Considerando 26 Directiva 95/46/CE: "*Considerando que los principios de la protección deberá aplicarse a cualquier información relativa a una persona identificada o identificable (...)*".

[519] Artículo 5.1.f) RDLOPD.

especialmente amplio a la definición. Hoy día está plenamente asumido que todos los datos que se refieren a una persona son en última instancia relevantes, por muy insignificantes que en un principio puedan parecer[520].

Esta amplitud en la caracterización de la información es un elemento importante, cuya razón de ser deriva directamente del debate creado a partir de la década de los 70 en torno a la necesidad de reconfigurar el derecho fundamental a la intimidad, y/o a la posibilidad de incorporar un nuevo derecho fundamental, el "derecho a la autodeterminación informativa", "el derecho a la libertad informática", o el "derecho a la protección de datos", al catálogo de los ya reconocidos.

Mucho se ha escrito sobre la conveniencia o no de aceptar la existencia de ese derecho como derecho autónomo al de la intimidad[521]. Una parte de la doctrina ha defendido con vigor la autonomía de ese derecho[522]. También el TC ha optado de forma contundente por esa posición[523]. Incluso en textos como la Carta de Derechos Fundamentales de la UE se reconoce la protección de datos como derecho con entidad propia, diferente al derecho a la intimidad[524]. Los defensores de esta interpretación se basan sobre todo en dos argumentos: que la intimidad sólo se refiere a lo íntimo, a lo más interno, no a toda la información relativa a una persona, y que consiste solamente en evitar que terceras personas accedan a ese espacio interno, no en un control positivo sobre la información concerniente a uno mismo, mientras que el nuevo derecho fundamental tendría un objeto de protección más amplio, y además abarcaría tanto facultades de exclusión como positivas de control.

Por el contrario, los autores que han abogado por no formular un nuevo derecho, han entendido que es suficiente con la revisión del derecho a la intimidad, de forma que éste pueda

[520] CARRASCOSA LÓPEZ, "La LORTAD...", cit., 1994, pp. 41-42, subraya que "es importante (...) cualquier dato, por insignificante que éste sea, ya que relacionado con otros puede poner en peligro la intimidad, pues como claramente pone de manifiesto el TC Federal Alemán, en sentencia de 15 de diciembre de 1983, ya no hay datos "sin interés"".

[521] TASCÓN LÓPEZ, *El Tratamiento por la Empresa…,* cit., 2005, pp. 33-50, realiza un interesante recorrido por las diferentes posiciones que han ido surgiendo en relación al derecho a la autodeterminación informativa; MARTÍNEZ MARTÍNEZ, *Una aproximación…,* cit., 2004, pp. 252-347.

[522] PÉREZ LUÑO, "Informática *y* Libertad...*",* cit., 1981; PÉREZ LUÑO, *Derechos Humanos...*, cit., 1991; PÉREZ LUÑO, *Intimidad y Protección...,* cit., 1992. MURILLO DE LA CUEVA, *El Derecho...*, 1990; MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, p. 24; MURIILO DE LA CUEVA, "La Construcción del Derecho…", cit., 2009, pp. 24-25. DEL CASTILLO VÁZQUEZ, *Protección de Datos…*, cit., 2007, pp. 239-241. HERRÁN ORTIZ, *El Derecho a la intimidad…,* cit., 2002, p. 87. PIÑAR MAÑAS, "Protección de Datos…", cit., 2009, p. 93; ARZOZ SANTISTEBAN, *Videovigilancia, seguridad…..,* cit., 2010, pp. 130-131.

[523] STC 30 de noviembre de 2000, FFJJ 4 y 5. Si bien es cierto que en anteriores resoluciones la autonomía del derecho a la autodeterminación informativa con respecto a la intimidad encontraban fundamento: STC 8 de noviembre de 1999, FJ 2: "la garantía de la intimidad adopta hoy un entendimiento positivo que se traduce en un derecho de control sobre los datos relativos a la propia persona; la llamada «libertad informática» es así derecho a controlar el uso de los mismos datos insertos en un programa informático («habeas data») y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención".

[524] Artículo 8 Carta de Derechos Fundamentales de la UE, 12 de diciembre de 2007: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.
3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

ampliar su objeto de protección y alcanzar a abrazar esa nueva esfera del individuo que, ante el avance de las nuevas tecnologías, ha de ser garantizado[525].

Independientemente de si esto es así o no, parece evidente que el ámbito de aplicación de las normas reguladoras del tratamiento de datos de carácter personal tiene que ser más amplio que el referido a lo estrictamente íntimo[526]. Efectivamente, se llame autodeterminación informativa, o libertad informática, o privacidad o intimidad[527], no hay duda de que lo que se quiere proteger en la LOPD no es lo estrictamente íntimo, sino toda la información relativa a una persona por muy insignificante que en un principio pueda parecer[528].

Esa relevancia que prácticamente la totalidad de la doctrina atribuye a esos datos en principio irrelevantes, se debe a que las nuevas tecnologías posibilitan una manipulación de la información que hasta ahora era absolutamente desconocida, haciendo viable la puesta en común de infinidad de datos originarios de muy diferentes ficheros, a una gran velocidad[529]. Datos que en un principio parecen insignificantes pueden ser puestos en común fácilmente con otros, pudiendo resultar de dicha relación perfiles completos de los individuos. El conocimiento por parte de la ciudadanía de estos nuevos medios tecnológicos, con los que se puede interceptar y utilizar información referida a los mismos, ha creado lo que se ha denominado como "síndrome de la pecera", "es decir, la psicosis que aqueja a los ciudadanos de vivir en una casa de cristal en la que todas las acciones pueden ser controladas"[530]. Esta situación ha hecho que sea necesario un marco normativo dirigido a la protección inmediata de cualquier información más allá de lo estrictamente íntimo[531].

---

[525] VILLAVERDE MENÉNDEZ, "Protección de Datos...", cit., 1994, p. 223; ORTÍ VALLEJO, *Derecho a la Intimidad...,* cit., 1994; GAY FUENTES, *Intimidad y tratamiento…,* cit., 1995, p. 29; REBOLLO DELGADO, *El Derecho...*, cit., 2005, p. 306; DE MIGUEL SÁNCHEZ, *Secreto Médico...,* cit., 2003, p. 269; MARTÍNEZ MARTÍNEZ, *Una aproximación crítica…,* cit., 2004, pp. 326-327.

[526] REBOLLO DELGADO, *El Derecho...,* cit., 2000, p.36: *"Intimus (a, um),* se traduce del latín por íntimo, el más íntimo. Su procedencia, la encontramos en el adverbio *intus,* traducible por dentro, o hacia dentro. Así, íntimo cabe traducirlo del término latino, como lo más interior, lo que tiende a demostrar la máxima interioridad". STC de 22 de abril 1993, FJ 7, reconoce que "el atributo más importante de la intimidad, como núcleo central de la personalidad, es la facultad de exclusión de los demás, de abstenerse de injerencias por parte de otro, tanto en lo que se refiere a la toma de conocimientos intrusivo, como a la divulgación ilegítima de datos".

[527] GUERRERO PICÓ, *El Impacto de Internet…*, cit., 2006, p. 187, señala las diferentes denominaciones que se otorga al derecho fundamental.

[528] STC 30 de noviembre del 2000, FJ 6, que zanja esta cuestión al reconocer que el derecho fundamental a la protección de datos protege cualquier tipo de dato personal, sea o no íntimo.

[529] HERRÁN ORTIZ, *El Derecho a la intimidad…,* cit., 2002, p. 53; MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 28; DAVARA RODRÍGUEZ, *Manual de Derecho...,* cit., 2003, p.43; GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, pp. 35-36; DEL CASTILLO VÁZQUEZ, *Protección de Datos…*, cit., 2007, p. 65.

[530] PÉREZ LUÑO, *Manual de Informática...,* cit., 1996, p.60. Tomemos como ejemplo la alarma social creada tras la afirmación por parte del Parlamento Europeo en Resolución del 2001 de la existencia de un sistema mundial de interceptación de comunicaciones, denominada red ECHELON, que no es otra cosa que una red de inteligencia de interceptación de comunicaciones.

[531] Se dice inmediata, porque, como nadie pone en duda hoy día, lo protegido de forma mediata es la "personalidad" del individuo, entendida como capacidad de disponer de su propia identidad, y fundamentada en última instancia en la dignidad del mismo. PÉREZ LUÑO, *Derechos Humanos...,* cit., 1986. En este sentido, son clarificadoras las palabras de OLIVER. y OLIVER, "Protección de Datos...", cit., 1994, nº 7, p. 250, quienes afirman que "la información sobre una persona constituye una especie de <<duplicado>> de la persona misma, su apariencia o configuración ante los demás, la realidad virtual con la que resulta, generalmente, identificada. Por eso, proteger los datos de una persona es proteger a la persona misma, defender sus derechos esenciales, los derechos de la personalidad". En la misma línea GARRIGA DOMÍNGUEZ, *La Protección...*, cit., 1999, pp.128-129, subraya que "la verdadera finalidad de la Ley no

V.1.3.La identificabilidad de la persona como límite.

De lo expuesto hasta ahora, resulta un concepto realmente amplio de la expresión "dato de carácter personal", entendiéndolo como todos los datos, no sólo los estrictamente íntimos, empleados con un fin determinado. Sin embargo, como no podía ser de otra forma, esta amplitud se ve limitada con la segunda parte de la definición. No basta con que se trate de cualquier información relativa a una persona, sino que hace falta que concierna a una persona identificada o identificable. Se trata de un matiz lógico, porque lo contrario podría llevar a soluciones realmente poco prácticas y absurdas como la de tener que aplicar la LOPD a los datos recogidos en las estadísticas. ¿Qué se entiende por persona identificada o identificable?

V.1.3.A. Referencia a la protección de los datos concernientes a la persona fallecida y al *nasciturus*.

En relación a lo que ha de entenderse por persona a la hora de aplicar la LOPD se pueden realizar las siguientes matizaciones. El CC considera que la personalidad se determina con el nacimiento[532] y se extingue por la muerte[533]. En la medida en que el derecho a la autodeterminación informativa es un derecho personalísimo, de la previsión del CC puede deducirse la imposibilidad de reconocer dicho derecho a favor de las personas fallecidas o el *nasciturus*. No se va a estudiar ahora esta cuestión de manera extensa, aunque hay que hacer algunos apuntes para comprender el alcance del concepto que se trata de aclarar.

A) Es un punto común afirmar que la titularidad de los derechos fundamentales comienza por la adquisición de la personalidad. Según el CC la personalidad se determina con el nacimiento. Por lo tanto, de inicio, el *nasciturus* no se considera titular de derechos fundamentales[534]. Así parece haberlo reconocido también la jurisprudencia cuando se ha enfrentado a la necesidad de decidir si el no nacido es titular del derecho a la vida o no, al negar la titularidad de dicho derecho, si bien reconociendo la necesidad de proteger objetivamente esa forma de vida[535]. Es cierto que a raíz de los problemas éticos y, también, jurídicos planteados en relación a la práctica del aborto y la necesidad de proteger de alguna forma la integridad del no nacido, en algún caso se ha planteado la posibilidad de reconocer la categoría de "vida humana" al *nasciturus,* llegando a cuestionar la validez de la citada previsión del CC, que podía atentar contra lo dispuesto en la

es proteger los datos personales de los ciudadanos, sino la protección de éstos en relación con el tratamiento automatizado de los mismos, para salvaguardar en último término la libertad de la persona y posibilitar su desarrollo sin interferencias".
En este sentido, llama la atención que la derogada Ley Orgánica 5/1992 y la vigente 15/1999, reguladoras en el Estado español del tratamiento de datos de carácter personal, no hayan hecho referencia en su encabezado a "la persona", como sí lo han hecho la Directiva 95/46/CE y el Convenio 108/1981 del Consejo de Europa, que se refieren a la protección de las personas en lo relativo al tratamiento de datos personales. DAVARA RODRÍGUEZ, *Manual de...*, cit., 2003, p. 50, resta importancia a este hecho. Sin embargo, se entiende aquí que la inclusión de una referencia expresa a la "persona" en el encabezado de las normas reguladoras del tratamiento de datos de carácter personal, como lo hacen la Directiva y el Convenio citados, hubiera dado la dimensión adecuada a dichas normas.

[532] Artículo 29 CC: "*El nacimiento determina la personalidad; pero el concebido se tiene por nacido para todos los efectos que le sean favorables, siempre que nazca con las condiciones que expresa el artículo siguiente*".

[533] Artículo 32 CC: "*La personalidad civil se extingue por la muerte de las personas*".

[534] GÓMEZ SÁNCHEZ, *Derechos y Libertades…,* cit., 2003, pp. 53-56.

[535] STC 11 de abril de 1985, FFJJ 6 y 7. GÓMEZ SÁNCHEZ, *Derechos y Libertades…,* cit., 2003, p. 157; ARENAS RAMIRO, *El Derecho Fundamental…*, cit., 2006, p. 458; DIEZ PICAZO, *Sistemas de Derechos…,* cit., 2008, p. 225.

Constitución en relación al derecho a la vida, pues esta norma no prevé nada sobre la necesidad de haber nacido para ser titular de dicho derecho[536]. Sin embargo, de la previsión realizada en el CC y por el TC, al vincular la personalidad al nacimiento, sería fácil negar la titularidad del *nasciturus* sobre el derecho a la autodeterminación informativa y, a su vez, negar la posibilidad de aplicar la normativa de protección de datos a favor de la información referida a esta figura.

En cualquier caso, si bien parece razonable negar la titularidad del derecho fundamental a la autodeterminación informativa al no nacido, ello no puede llevar a la desprotección absoluta de los datos que a él se refieren. Se entiende aquí que resulta conveniente reconocer la necesidad de proteger objetivamente los datos de carácter personal concernientes al *nasciturus*[537], atendiendo a los siguientes argumentos.

Desde las normas cabe encontrar justificación a lo defendido aquí. El CC afirma que "*el concebido se tiene por nacido para todos los efectos que le sean favorables, siempre que nazca con las condiciones que expresa el artículo siguiente*". Determinar el contenido de dicho precepto y el alcance de la capacidad jurídica del *nasciturus* ha generado cierta polémica en la doctrina[538]. En algunos casos se ha pretendido realizar una interpretación restrictiva de este precepto, señalando que los efectos favorables no se refieren a los derechos fundamentales sino, solamente, a facultades que derivan del ámbito patrimonial[539]. En lo que aquí interesa, más allá de que pueda plantearse o no la titularidad de este sujeto del derecho a la autodeterminación informativa, la aplicabilidad de las reglas de protección de datos a la información concerniente al *nasciturus* no plantea demasiadas dudas. El Grupo de Trabajo del artículo 29 de la Directiva europea afirma que, en los estados en que se atribuye la titularidad de los citados derechos o facultades patrimoniales a los no nacidos, no puede haber duda sobre el reconocimiento también de la necesidad de proteger los datos que les conciernen[540]. La Recomendación del Consejo de Europa sobre la protección de datos médicos va más allá reconociendo expresamente la necesidad de proteger la información a la que ahora se hace referencia[541]. Partiendo de estas previsiones la doctrina ha reconocido de manera acertada la necesidad de proteger los datos de carácter personal referidos al no-nacido[542].

---

[536] DIEZ PICAZO, *Sistemas de Derechos…,* cit., 2008, p. 226.

[537] ROMEO CASABONA, "Persona identificada…", cit., 2010, p. 243, expone argumentos a favor de la aplicación de la normativa de protección de datos a los no-nacidos.

[538] O´CALLAGHAN, "El Concebido…", cit., 2004.

[539] ARROYO i AMAYUELAS, *La Protección…,* cit., 1992, p. 104. De hecho, las principales referencias al concebido pero no nacido en el CC conciernen al campo patrimonial: Artículo 627 CC: "*Las donaciones hechas a los concebidos y no nacidos podrán ser aceptadas por las personas que legítimamente los representarían, si se hubiera verificado ya su nacimiento*". Artículo 966 CC: "*La división de la herencia se suspenderá hasta que se verifique el pacto o el aborto, o resulte por el transcurso del tiempo que la viuda no estaba encinta. Sin embargo, el administrador podrá pagar a los acreedores, previo mandato judicial*". En relación a esta cuestión MATA DE ANTONIO, "Problemas Prácticos…", cit., 2003.

[540] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007.

[541] Artículo 4.5 R (97) 5: "*Los datos médicos relativos a niños no nacidos deben considerarse datos personales y gozar de una protección comparable a la de los datos médicos de un menor*". SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000, p. 111; SOLERNOU VIÑOLAS, "Aspectos legales y éticos…", cit., 2005, p. 53.

[542] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, p. 175; GÓMEZ-JUÁREZ SIDERA, "Breve reflexión…", cit., 2007.

Lo dicho encuentra también apoyo en la práctica. En lo que concierne a los datos de salud, hay que tener en cuenta, por un lado, que de esa información referida al *nasciturus* resulta inevitablemente información sobre la salud de la misma persona una vez ha nacido. Los adelantos tecnológicos permiten hoy día extraer gran cantidad de información sobre el no nacido. Estos datos aproximan mucho una idea sobre cómo será la salud de la persona después de que haya nacido. Por otro lado, la información del *nasciturus* puede afectar a terceras personas biológicamente vinculadas a él. La protección de los datos del *non nato* se entiende necesaria, por lo tanto, por cuanto que supone la protección de información relativa a personas físicas ya nacidas.

B) En lo que corresponde al fallecido, la normativa reguladora de la protección de datos en el ámbito estatal otorga argumentos para negar la aplicabilidad de estas normas a los datos concernientes a los sujetos fallecidos. Si bien la Ley no dice nada al respecto, el RDLOPD niega la aplicabilidad de dicho reglamento a la información de las personas fallecidas[543]. Se ha llegado a afirmar que no son titulares del derecho a la autodeterminación informativa[544]. Sin embargo, y como se verá con mayor profundidad al analizar la cesión de los datos sanitarios, existen argumentos suficientes para concluir que este tipo de información es también objeto de protección por la normativa de protección de datos, cuando menos en el sector sanitario[545].

La LBAP, por ejemplo, protege expresamente la intimidad de las personas fallecidas[546]. También lo hace la Ley orgánica 1/1982, al reconocer que la persona designada por el fallecido será la encargada de proteger la intimidad, entre otros derechos, de aquél[547]. Las agencias de

[543] Artículo 2.4 RDLOPD: "*Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos*". TRONCOSO REIGADA, "*La protección de datos…*", cit., 2008, p. 27, critica el hecho de que el reglamento limite la titularidad del derecho fundamental a la autodeterminación informativa cuando no lo hace la Ley; APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 64, en el mismo sentido.

[544] Informe jurídico AEPD, 61/2008.

[545] PUENTE ESCOBAR, "Ámbito objetivo…", cit., 2008, p. 60.

[546] Artículo 18.4 LBAP: "*Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros*"

[547] Artículo 4 LO 1/1982, de 5 de mayo de 1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen: "*1. El ejercicio de las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida corresponde a quien ésta haya designado a tal efecto en su testamento. La designación puede recaer en una persona jurídica.*

2. No existiendo designación o habiendo fallecido la persona designada, estarán legitimados para recabar la protección el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento.

3. A falta de todos ellos, el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio, a la instancia de persona interesada, siempre que no hubieren transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento". Artículo 6: "*1. Cuando el titular del derecho lesionado fallezca sin haber podido ejercitar por sí o por su representante legal las acciones previstas en esta ley, por las circunstancias en que la lesión se produjo, las referidas acciones podrán ejercitarse por las personas señaladas en el artículo cuarto.*

protección de datos también han adoptado una postura relativamente abierta en este sentido. Las memorias de la AEPD han reconocido que la protección de los derechos a la intimidad y al honor subsisten incluso después de la muerte de las personas[548]. La AVPD por su parte ha señalado que la protección de los datos de las personas fallecidas es necesaria, por cuanto que estos datos, e incluso el propio dato del fallecimiento, pueden afectar a terceros que debido a dicho hecho se convierten en titulares de derechos y obligaciones[549]. Los tribunales han reconocido que ciertos hechos ocurridos a personas cercanas a un sujeto pueden afectar a la esfera de la personalidad de este último[550]. Esta consideración es especialmente importante en el ámbito sanitario, en el que la información sobre la salud de una persona fallecida puede reflejar datos sobre la salud de personas vinculadas a ella[551]. Parece que una cosa es que los fallecidos no sean titulares del derecho a la autodeterminación informativa y otra que los datos relativos a un fallecido no sean objeto de protección alguna[552].

En conclusión, y a efectos de definir el concepto de dato de carácter personal, habrá que entender la "persona" en un sentido relativamente amplio. Podría debatirse también la aplicabilidad de esta normativa a los datos concernientes a las personas jurídicas, pero tratándose este trabajo sobre la protección de datos sanitarios su estudio no ofrece especial interés[553].

V.1.3.B. La necesidad de que la identidad de la persona sea determinada o determinable.

El aspecto de análisis más importante en este epígrafe lo constituye la referencia en la definición a que el dato ha de concernir a una persona identificada o identificable. Es necesario precisar cuándo se da esta circunstancia. Frente a la calificación de unos datos como referidos a una persona identificable se encuentran los datos disociados, entendiendo este concepto en un

---

2. Las mismas personas podrán continuar la acción ya entablada por el titular del derecho lesionado cuando falleciere".

[548] Memoria de la AEPD 2002, p. 314.

[549] Dictamen de la AVPD, CN06-013.

[550] STC 25 de noviembre de 1996, FJ 2, en la que se apunta que la publicación de la adicción a las drogas de una persona fallecida puede afectar al derecho al honor de sus familiares.

[551] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007, pone de manifiesto este hecho, subrayando la importancia de los datos genético.

[552] MESSÍA DE LA CERDA BALLESTEROS, "Personalidad y protección…", cit., 2008.

[553] Artículo 2.2 RDLOPD: "*Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales*". Informe jurídico AEPD, 0038/2010, en el que se niega la aplicabilidad de la Ley a las personas jurídicas. NAVALPOTRO NAVALPOTRO, "Ámbito de aplicación…", cit., 2007, p. 79; GUICHOT, *Datos Personales…,* cit., 2005, p. 186. STS 20 de febrero de 2007, FJ 6, en la que se sobreentiende que las personas jurídicas no son titulares del derecho de protección de datos. El TEDH parece haber adoptado otro camino, reconociendo a las personas jurídicas la posibilidad de ejercer determinadas facultades del derecho a la autodeterminación informativa para proteger, fundamentalmente, datos de carácter económico de los que dichas personas jurídicas son titulares SSTEDH 16 de diciembre de 1992, caso Niemitz; 25 de febrero de 2003, caso Roemen and Schmit. Esta línea podría tener entrada en el ámbito interno, en lo que toca al ámbito del derecho a la autodeterminación informativa, partiendo de decisiones como STC 2 de febrero de 1989, FJ 2, en la que se reconoce, tempranamente, que "(…) en nuestro ordenamiento constitucional aun cuando no se explique en los términos con que se proclama en los textos constitucionales de otros Estados, los derechos fundamentales rigen también para las personas jurídicas nacionales en la medida en que, por su naturaleza, resulten aplicables a ellas. Así ocurre con el derecho a la inviolabilidad del domicilio, o el derecho a la tutela judicial efectiva".

sentido amplio que engloba todos aquellos datos que no permiten la identificación de los titulares de los mismos[554].

La identidad hace referencia a los rasgos que caracterizan a un individuo frente a todos los demás, bien sea atendiendo a características fisiológicas, económicas, sociales o culturales[555]: nombre y apellidos, DNI, Nº de la Seguridad Social, ADN, entre otros. Cuando una información pueda vincularse con cualquiera de estos rasgos identificativos se entenderá que se está ante información de carácter personal a efectos de aplicar la LOPD. En estos casos no hay problema alguno sobre la aplicabilidad de la Ley pues la relación entre la información y la identidad es directa. Los problemas comienzan cuando la información se refiere a una persona cuya identidad no se puede determinar de forma tan clara como en esos casos, pero que puede llegar a ser concretada cruzando archivos, realizando investigaciones etc. Ya se ha advertido en numerosas ocasiones sobre la existencia de manipulaciones que, empleando sobre todo la informática, convierten datos en principio anónimos en fichas completas relativas a personas identificadas[556]. La cuestión principal radicará en determinar cuándo se entiende que una persona es identificable[557].

La LOPD no dice nada al respecto. Antes de la aprobación del RDLOPD era el reglamento que desarrollaba la LORTAD el que fijaba qué había de entenderse por identificable[558]: "*cualquier elemento que permite determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada*"[559]. Se trataba de una definición realmente amplia que reproduce prácticamente en los mismos términos la Directiva europea[560]. La amplitud de esta definición fue alabada por parte de la doctrina por entender que llegaba a

[554] Artículo 3.f) LOPD: "*Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable*"; Artículo 5.1.e) RDLOPD; Considerando 26 Directiva 95/46/CE: "*(...) que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado (...)*".Informe jurídico AEPD, 207/2008. SAN 8 de marzo de 2002, FJ 5, señala que el proceso de disociación "consiste en eliminar la conexión entre el dato y la persona, en "despersonalizar" el dato, actuando como barrera que impide la identificación y entrañando en definitiva un elemento protector de la intimidad o privacidad del afectado". Tanto desde las leyes como, desde la doctrina se han hecho distinciones entre datos anónimos, disociados o datos no-personales. A pesar de que esta diferenciación tiene pleno sentido, se entiende que en este trabajo es suficiente con la consideración de datos disociados como contrapunto al dato de carácter personal: MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 34; NICOLÁS JIMÉNEZ, *La Protección Jurídica…*, cit., 2006, p. 63. Esta distinción tiene apoyo en la actualidad en Artículo 3 Ley 14/2007, 3 de julio, de Investigación Biomédica: "*h) Dato anónimo: dato registrado sin un nexo con una persona identificada o identificable; i) Dato anonimizado o irreversiblemente disociado: dato que no puede asociarse a una persona identificada o identificable por haberse destruido el nexo con toda información que identifique al sujeto, o porque dicha asociación exige un esfuerzo no razonable, entendiendo por tal el empleo de una cantidad de tiempo, gastos y trabajo desproporcionado*"; APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 72, también se refiere a esta distinción.

[555] ROMEO CASABONA, "Persona identificada…", cit., 2010, p. 227.

[556] Memoria de la AEPD 2000.

[557] Artículo 13.2 Ley 12/1989 de 9 de mayo de la Función Estadística Pública: "*Son datos personales los referentes a personas físicas o jurídicas que o bien permiten la identificación inmediata de los interesados o bien conduzca por su estructura, contenido o grado de desagregación a la identificación (...)".*

[558] CARDONA RUBERT, *Informática y Contrato...*, cit., 1999, p.103.

[559] Artículo 1.5 RD 1332/1994.

[560] Artículo 2.a) Directiva 95/46/CE: "*(...) se considera identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, cultural o social*".

abarcar todos los datos posibles que pudieran relacionarse con una persona, bien de forma directa o bien de manera indirecta[561]. De esta manera se subrayaba la inclusión en la definición del término "indirectamente", pues ampliaba la aplicabilidad de la Ley incluso a los supuestos en que la identificabilidad de la persona fuera remota[562].

Sin embargo, esta interpretación podía contraponerse con una visión más restrictiva del concepto. En algunos textos normativos la identificabilidad se entiende de manera más estricta. La propia Directiva europea se hace eco en sus considerandos de la necesidad de que la identificabilidad se vincule con los medios con que se cuenta para poder relacionar la información con el titular de los datos[563]. El Consejo de Europa considera, al interpretar el Convenio de 1981, que la persona identificable se refiere a aquella que puede ser fácilmente identificable, dejando a un lado los supuestos en que la identificación requiere métodos muy sofisticados para su realización[564]. La misma línea sigue la Recomendación del Comité de Ministros del Consejo de Europa relativo al Uso de Datos Personales con Fines de Investigación Científica y Estadística, pero precisando algo más los criterios empleados para considerar si una persona es o no identificable. Así, no se considerará que una persona es identificable cuando esta operación requiere una cantidad irracional de "tiempo, coste y esfuerzo"[565]. Este criterio, que se mantiene como fundamento para determinar la identificabilidad de la persona en posteriores recomendaciones del mismo organismo[566], cambia en la fundamental Recomendación del Comité de Ministros del Consejo de Europa sobre Protección de Datos Médicos en la que establece que los criterios a tener en cuenta para determinar la identificabilidad son "el tiempo y los medios empleados", dejando a un lado "los costes". En la memoria explicativa de la citada Recomendación se considera que, si se tienen en cuenta los avances de la informática, el aspecto de los costes no es fiable a la hora de determinar si una persona es identificable o no. Efectivamente, el coste económico de los medios que se pueden emplear para la identificación de una persona no es un criterio fiable, ya que hoy día muchos de esos medios son realmente accesibles. No hay más que ver el incremento constante del número de usuarios de internet, que constituye una herramienta de gran alcance a la hora de concretar la identidad de sujetos determinados. En definitiva, habría que atender a criterios "temporales" y "de esfuerzo" para determinar si una persona es o no identificable[567].

[561] MUNAR BERNAT, "El Tratamiento...", cit., 1997, p.106.
[562] DAVARA RODRÍGUEZ, *La Protección...,* cit., 1998, p.47, afirma que queda "claro que la Directiva pretende que la protección se extienda a toda persona que, de una forma u otra, por asociación de conceptos o contenidos, aunque no se haga referencia directa a ella, pueda ser identificada o identificable".
[563] Considerando 26 Directiva 95/46/CE: "*(...) para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona*".
[564] Memoria Explicativa del Convenio 108/1981 del Consejo de Europa, 108/81, 28 de enero de 1981.
[565] Artículo 1.2 Recomendación Nº R(83) 10 del Comité de Ministros del Consejo de Europa relativo al Uso de Datos Personales con Fines de Investigación Científica y Estadística, adoptada el 23 de septiembre de 1983: "*An individual should not be regarded as "identifiable" if the identification requires an unreasonable amount of time, cost and manpower*" (Esta Recomendación ha sido sustituida por la R(97) 18 de 20 de septiembre). http://www.coe.int/.
[566] Recomendación R (86) 1 del Comité de Ministros del Consejo de Europa para la Protección de Datos Personales empleados con Fines de Seguridad Social, adoptada el 23 de enero de 1986.
[567] Así lo recoge también el art. 1.a) de la reciente Recomendación R (02) 9 del Comité de Ministros del Consejo de Europa sobre la Protección de Datos Recogidos y Tratados a efectos de Seguros, adoptada el 18 de septiembre de 2002.

Podría plantearse, por lo tanto, atendiendo a diferentes textos jurídicos, la necesidad de optar por una u otra interpretación: entre considerar por identificable toda persona cuya identidad puede, de una u otra forma, ser determinada, o comprender sólo las personas que puedan ser identificables empleando tiempo y esfuerzo razonables[568]. Hoy día el RDLOPD zanja este debate al adoptar la segunda postura, añadiendo a la definición que daba el anterior reglamento que desarrollaba la LORTAD la necesidad de que la identificación de la persona no requiera de plazos o actividades desproporcionadas[569]. El mismo criterio se sigue en la Ley de Investigación Biomédica, si bien vuelve a incluir el criterio económico para determinar si la identificabilidad es posible o no[570]. Antes de la aprobación del RDLOPD, la propia AEPD[571] y la jurisprudencia[572] habían puesto de manifiesto la necesidad de entender el concepto "identificable" en un sentido no demasiado amplio. Merece la pena aclarar los argumentos que han llevado a justificar tal interpretación.

Se entiende aquí que en última instancia toda información relativa a una persona puede, de una u otra forma, relacionarse con la identidad del sujeto concreto al que se refiere, en la medida en que toda información cierta sobre una persona se conoce siempre a través de una fuente determinada (la propia persona, terceros, etc.) a la que con mayor o menor esfuerzo y tiempo se puede llegar. No es correcto entender el concepto identificable en términos absolutos, sin ningún tipo de limitación. Esta interpretación llevaría a considerar todo tipo de información como identificable, incluso la estadística. Sería difícil hablar de datos disociados. Si no fuera necesario que la relación entre el dato y la identidad del titular del mismo fuera cercana, se acabaría entendiendo que la normativa de protección de datos es aplicable a todo tipo de información, a pesar de que en un principio pudiera parecer que se refiere a un sujeto no identificable.

Es por esto que el término identificable hay que interpretarlo como razonablemente identificable. Una persona será identificable cuando la búsqueda de dicha identidad no requiera un esfuerzo absolutamente desproporcionado[573]. De esta forma, para determinar si efectivamente se trata de un dato referido a un sujeto identificable o no, deberá atenderse a los medios con los que puede contar el sujeto que quiere llevar a cabo la manipulación de la información.

Siendo correcta la afirmación de que la identificabilidad ha de ser posible mediante el empleo de tiempo y esfuerzo razonables, lo cierto es que la aplicación de esta interpretación puede resultar en la práctica problemática. Esto se debe a que la indeterminación de los términos "esfuerzo y tiempo razonables" podría abrir las puertas a una utilización discrecional de este

[568] GÓMEZ PIQUERAS, "Anonimización y disociación…", cit., 2009, p. 15, hace un interesante análisis sobre cuándo unos datos son identificables y cuándo disociados o anonimizados.
[569] Artículo 5.1.o) RDLOPD: "*Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados*".
[570] Artículo 3.i) Ley 14/2007, 3 de julio, de Investigación Biomédica.
[571] *Conclusiones y recomendaciones de la APD, de la inspección sectorial de oficio de "Concursos, juegos y sorteos de Televisión",* http://www.agpd.es/. Informe jurídico AEPD, 0082/2010, que hace suyo el criterio adoptado por el reglamento.
[572] SAN 8 de marzo de 2002, FJ 5.
[573] NICOLÁS JIMÉNEZ, *La Protección Jurídica…*, cit., 2006, p. 65. DEL CASTILLO VÁZQUEZ, *Protección de Datos…*, cit., 2007, p. 336; ROMEO CASABONA, "Persona identificada…", cit., 2010, pp. 234-235.

concepto. En este sentido se ha señalado en alguna ocasión que el criterio aportado, y que ahora se recoge en el RDLOPD, resulta impreciso, pues no se establecen los parámetros suficientes a la hora de definir cuándo se requiere un esfuerzo desproporcionado y cuándo no[574].

Si bien es verdad que se trata de un criterio que puede generar cierta inseguridad, no se comparte la idea de que es poco acertado. Se ha concluido que es necesario limitar la consideración de dato de carácter personal a los casos en que la información se refiere a persona identificable mediante el uso de medios razonables, ya que lo contrario puede llevar a un régimen excesivamente garantista y poco práctico. La identificabilidad ha de ser posible mediante el empleo de tiempo y esfuerzo razonables. El hecho de que el criterio empleado para dicha limitación sea amplio responde a la necesidad de adaptarse al momento histórico concreto, como ha ocurrido con el criterio de los costes, que anteriormente parecía válido pero que hoy ha dejado de tener relevancia[575]. El establecimiento de parámetros más limitados podría cerrar las puertas a nuevos supuestos de identificabilidad. Siendo cierto que podía haberse establecido una lista orientativa con ejemplos de lo que se considera por "plazos y actividades desproporcionados", se entiende que en este caso el legislador ha establecido un criterio amplio, flexible, pero lo suficientemente delimitable, excluyendo sólo los supuestos en los que haga falta un uso de tiempo y esfuerzo desproporcionados para identificar a la persona a la que se refiere la información, cosa que habrá que apreciar caso por caso.

Para comprender lo que se acaba de señalar puede atenderse a supuestos concretos en que se han planteado dudas sobre la consideración de unos datos como referidos a personas identificables. Hay casos en que no hay problema a la hora de resolver dichas dudas. Un supuesto claro de identificabilidad podría constituir la referencia en un tablón, en el portal de una comunidad, de la consideración de moroso de quien vive en un piso y puerta determinada. La referencia al piso y a la puerta es evidentemente dato de carácter personal[576]. En otros casos, sin embargo, los problemas son mayores. Se ha planteado, por ejemplo, si los números de teléfono, sin referencia alguna a la identidad de los titulares de dichas líneas, constituyen datos de carácter personal. En un informe jurídico la AEPD ha considerado que no, debido a que se trata de información que no es vinculable con la identidad de los titulares de los datos[577]. En otro informe, sin embargo, la propia Agencia ha reconocido que un listado de teléfonos puede considerarse como dato de carácter personal en la medida en que están asociados a una dirección concreta, a pesar de que no se conozca la identidad del titular[578]. En el caso de una lista de números de teléfonos, si bien es cierto que de inicio se trata de información no vinculada a personas determinadas, no se puede desatender la idea de que en la actualidad no exige esfuerzos desproporcionados conocer, partiendo de dicho número, al titular de la línea: bien empleando

[574] LEGALIA, *La Protección...*, cit., 2002, pp. 51-52; FERNÁNDEZ LÓPEZ, "Algunas Reflexiones…", cit., 2007, p. 41, critica el que el nuevo reglamento que desarrolla la LOPD emplee estos términos indeterminados.
[575] MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 33.
[576] Resolución de la AEPD R/00579/2008, 23 de mayo de 2008. Procedimiento PS/00427/2007. Lo mismo ocurre cuando, por ejemplo, se aportan datos sobre una persona que ocupa un puesto de trabajo en un ayuntamiento y sólo hay un único sujeto que ocupe dicho puesto. A pesar de que la información aparezca disociada será muy fácil deducir quién es el titular de los datos, teniendo en cuenta que sólo hay una persona en el puesto de trabajo al que se hace referencia: SAN 29 de abril de 2010, FJ 1.
[577] Informe jurídico AEPD, 0575/2008.
[578] Informe jurídico AEPD, 285/2006.

medios informáticos o, incluso, llamando directamente al propio número. La Agencia en otros informes parece adoptar una posición más garantista al reconocer que hay identificabilidad en listados de dígitos de identificación de animales, debido a que a partir de dichos dígitos puede conocerse la identidad de los dueños en los Registros de animales de compañía[579], o al reconocer la misma consideración de los números de las matrículas de los vehículos, debido a la posibilidad de determinar la identidad de los titulares a través del Registro de vehículos[580].

Se entiende aquí que el que se podría llamar como juicio de identificabilidad habrá que realizarlo en cada caso, atendiendo al contexto en que se van a emplear dichos datos. Y es que si se realiza una interpretación especialmente estricta de lo que ha de interpretarse por identificable puede llegar a entenderse, por ejemplo, que el número de una historia clínica no es un dato de carácter personal. Si bien de inicio puede ser así, según las circunstancias en que se empleen dichos números podrán o no considerarse datos de carácter personal. Si dichos números son empleados dentro de un sistema sanitario parece necesario que sí sean considerados como datos de carácter personal, pues la identificabilidad de los titulares es, efectivamente, posible e incluso necesaria[581]. La identificabilidad hay que determinarla atendiendo a las circunstancias concretas en que se manipule la información: el contexto en que se haga y la posibilidad que se tiene de relacionar los datos, que en principio no se refieren a un sujeto identificable, con otros que pueden traer como resultado la identificación del titular[582].

Tomando en consideración lo antedicho se puede afirmar que cuando se habla de "dato de carácter personal" se hace referencia a todo dato, no sólo del estrictamente íntimo, empleado con un determinado fin, entendiendo el término fin en sentido amplio, que se refiere a persona cuya identidad puede ser concretada con el empleo de tiempo y esfuerzo razonables o proporcionados.

V.1.4.La diferencia entre el "dato personal" y el "dato de carácter personal". La consideración de las evaluaciones y apreciaciones sobre las personas como datos de carácter personal.

Hasta ahora se ha estado hablando de los datos de carácter personal. Sin embargo, si se atiende al articulado de la LOPD, se observará que este concepto se alterna con el de dato personal[583]. ¿Se trata realmente de fórmulas sinónimas? Esta cuestión ha sido resuelta por la jurisprudencia y la doctrina con acierto, al concluir que el dato de carácter personal y el dato personal, aunque a veces son coincidentes, no siempre se refieren a la misma realidad[584].

[579] Informe jurídico AEPD, 319/2008.
[580] Informe jurídico AEPD, 425/2006.
[581] Informe jurídico AEPD, 0283/2008. Señala que, a pesar de que los números de las historias corresponden a un proceso de disociación, en la medida en que tras él la identidad de la persona titular de la información contenida en las historias queda oculta, esta disociación no es plena a efectos de la aplicación de la LOPD, por cuanto que en el ámbito sanitario la posibilidad de relacionar la identidad de dichas personas con los números de las historias es alta y no exige esfuerzos desproporcionados.
[582] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007, pone el ejemplo de un apellido que, en un inicio, puede ser muy común en un pueblo de forma que no constituiría por sí mismo un elemento identificable, pero que, sin embargo, ese mismo apellido empleado en un ámbito más reducido, como puede ser una clase en una escuela, sí constituye un elemento identificable.
[583] En los cuatro primeros artículos de la LOPD, el legislador emplea varias veces los dos conceptos como sinónimos.
[584] STS 31 de octubre del 2000, FJ 2. SEOANE RODRÍGUEZ, "De la Intimidad... ", cit., 2002, pp. 137-140. NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, p. 63.

Desde el punto de vista sustantivo el dato de carácter personal tiene un alcance mayor que el dato personal. Este último se refiere a la información concerniente a la persona considerada en sí misma: nombre y apellidos, número de DNI, etc[585]. La jurisprudencia entiende que el concepto de datos de carácter personal, en contraposición con el de dato personal, engloba "a)los datos personales *strictu sensu*, que son aquellos datos existenciales que pueden ser asociados a una persona determinada o determinable (nacimiento, muerte, matrimonio, domicilio y análogos), los datos referentes a la actividad profesional, al patrimonio, a la pertenencia a una confesión religiosa, a un partido político, las enfermedades, etc., b)La <<información sobre las condiciones materiales>>, concepto que quedaría englobado dentro de la ambigua frase empleada por el art. 3. Letra a) LORTAD: <<cualquier información>>, c) Evaluaciones y apreciaciones que puedan figurar en el fichero y que hagan referencia al afectado" [586].

Es de especial interés observar que el TS ha incluido las evaluaciones y apreciaciones que puedan figurar en el fichero y que hagan referencia al afectado en el concepto de dato de carácter personal. En algún caso la doctrina ha considerado que la definición dada en la Ley a los datos de carácter personal se refiere a los datos objetivos, materiales, sobre la persona y no a las valoraciones que puedan desprenderse de dichas informaciones[587]. Así parece que lo han entendido también en algún momento los Tribunales, refiriéndose concretamente a información contenida en una Historia Clínica[588].

Es cierto que cuando dichas apreciaciones subjetivas no son más que meras opiniones personales es impensable aplicar la LOPD. Piénsese en un fichero que contiene únicamente valoraciones subjetivas de determinadas personas, sin referencia alguna a información objetiva de las mismas, y que tiene como fin la mera expresión de dichas apreciaciones. Sin embargo, hay que tener en cuenta que hay supuestos en que esas evaluaciones son algo más que una mera opinión, llegando a constituir un fundamento para la toma de decisiones por terceros, que pueden afectar al titular de dicha información. Es lo que ocurre por ejemplo en el ámbito sanitario, en el que los profesionales se tienen que basar en apreciaciones subjetivas para la toma de decisiones que afectarán directamente a los pacientes[589]. Se trata de casos en que la valoración, aunque no sea información objetiva sobre la persona, es tratada como tal, empleándose con fines determinados que afectan a la persona a la que se refiere. No parece adecuado que sobre esta apreciación el interesado no tenga los derechos reconocidos en la LOPD[590]. En este sentido, la

[585] RUIZ CARRILLO, *La Protección de los Datos…,*cit., 2001, p. 21.
[586] STS 31 de octubre del 2000, FJ 2.
[587] CARDONA RUBERT, *Informática y Contrato...*, cit., 1999, p.144.
[588] SAP de Alicante, 6 de julio de 2001, FJ 3, señala que "la Historia Clínica comprende no sólo datos objetivos, que esos sí deben serle entregados al paciente que los reclama sobre la atención recibida, sino además datos personales y propios de estudios, hipótesis, impresiones plasmadas en papel, etc. que no pertenecen al paciente sino al profesional que lo atendió". Si bien, es cierto, esta resolución puede ser fruto, no de la consideración de que los datos subjetivos no son datos de carácter personal, sino de entender que existe un interés jurídico de mayor relevancia que el derecho a la autodeterminación informativa del paciente.
[589] MURILLO DE LA CUEVA, "El Derecho Fundamental...", cit., 2005.
[590] Es por lo tanto altamente cuestionable lo establecido por el artículo 18.3 de la Ley 41/2002: "*El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas".* MARTÍNEZ AGUADO, "Aspectos éticos…", cit., 2001, p. 90,

propia LOPD reconoce en su articulado el derecho de acceso del interesado sobre las posibles evaluaciones y apreciaciones que sobre su persona se hayan realizado en los ficheros sobre solvencia patrimonial y crédito[591]. En la medida en que recoge la posibilidad de ejercer este derecho sobre ese tipo de valoraciones, aunque se refiera a ficheros concretos, parece estar reconociendo la aplicabilidad en algunos casos a este tipo de información. Es, por lo tanto, necesario integrar este tipo de información "subjetiva" en el ámbito de actuación del concepto de dato de carácter personal[592].

Desde el punto de vista material, por lo tanto, se ha reconocido la mayor amplitud del concepto "dato de carácter personal": no todos los datos de carácter personal son datos personales. Sin embargo, desde un aspecto más formal el TS ha observado que no todos los datos personales son datos de carácter personal. Los datos de carácter personal son una variedad de los otros en el siguiente sentido: los denominados datos personales pueden serlo sin tener "carácter personal" en la medida en que pueden no referirse a una persona determinada o determinable[593]. Así pues, los datos personales serán de carácter personal, cuando se refieran a una persona determinada o determinable.

En resumen, se puede concluir que, tanto desde el punto de vista sustantivo como formal, los conceptos "dato de carácter personal" y "dato personal" se refieren a realidades diferentes. Sin embargo, y atendiendo al uso alternativo que la LOPD realiza de ambos, habrá que entender a efectos prácticos que se emplean como tal, pues no parece que haya estado en la voluntad del legislador realizar ninguna distinción entre los mismos.

V.2.El dato de carácter personal relativo a la salud.

Una vez aclarado lo que se ha de entender por dato de carácter personal es necesario dar un paso más y analizar lo que ha de interpretarse por dato relativo a la salud. En las líneas siguientes se tratará de determinar el significado de conceptos como el dato relativo a la salud, el dato sanitario o el dato sometido a una protección especial, con el fin de concretar su alcance.

V.2.1.Definición del concepto "dato relativo a la salud". La distinción entre "dato sanitario" y "dato relativo a la salud".

En la relación entre paciente y todo el personal que se integra en el ámbito sanitario, tanto médico como administrativo, se produce necesariamente un flujo de información relativa al

señala la posibilidad de que el paciente tenga acceso a la información objetiva de la historia clínica, pero no a la parte subjetiva.

[591] Artículo 29.3 LOPD: *"En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos"*

[592] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2007, sobre el concepto de datos personales, 20 de junio de 2007, en el que se hace mención a la importancia de este hecho en ámbitos como el laboral o el de la banca, donde apreciaciones de este tipo llevan a tomar decisiones que afectan a los titulares de los datos.

[593] HEREDERO HIGUERAS, *La Ley...*, cit., 1996, p.71, entiende que los datos personales "pueden constituir una masa de datos <<sin carácter personal>>, si no pueden ser asociados a una persona determinada o determinable"; SEOANE RODRÍGUEZ, "De la Intimidad genética...", cit., 2002, p. 144; MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 32.

usuario o paciente, que englobará datos de muy distinto contenido y sensibilidad pero cuyo tratamiento será necesario para llevar a cabo el servicio sanitario.

Datos que aportará el propio paciente, los que aportarán fuentes distintas a éste y la información que deducirá el propio profesional sanitario, constituirán un cuerpo informativo que abarcará desde informaciones en principio irrelevantes, como pueden ser la edad o el domicilio, hasta datos que la mayoría de las personas entienden que afectan a la esfera más interna de cada uno, como puede ser la relativa a la vida sexual o a una enfermedad determinada.

En los sistemas sanitarios se crean ficheros que contienen gran cantidad de datos. En la mayoría de casos en estos ficheros se distinguen diferentes categorías de datos. Por ejemplo, el fichero de Osakidetza denominado Registros de Casos de Sida se estructura de la siguiente manera: Datos identificativos; Datos de características personales; Datos de circunstancias sociales, tales como aficiones y estilo de vida; y, Datos especialmente protegidos, haciendo referencia en este último apartado a los datos de salud y los relativos a la vida sexual[594]. En este fichero se hace referencia expresa a los datos de salud. Por lo tanto, se podría deducir de esta resolución que son datos de salud los estrictamente médicos, mientras que los demás no adquirirían esta consideración. Por otro lado se mencionan los datos especialmente protegidos, aplicándose este calificativo de manera exclusiva a los datos puramente médicos y a los relativos a la vida sexual. Resulta necesario aclarar estos conceptos para conocer el alcance real de normas como la que se acaba de citar.

La heterogeneidad en la información contenida en los distintos ficheros que se emplean en el sector sanitario hace necesario, que se pregunte a qué se hace referencia cuando se habla de los datos de carácter personal relativos a la salud, teniendo presente que la consideración de unos datos como tales, les otorgará por los artículos 7 y 8 LOPD una regulación particular.

Si se acude a la LOPD se observará que no se da una definición del concepto “dato relativo a la salud”, como tampoco se da en la Directiva europea. Estas normas, como bien apunta la doctrina, solamente se dedican a otorgar una mínima regulación de este tipo de información[595]. Es más, si se atiende exclusivamente al artículo 8 LOPD se podría deducir que los datos relativos a la salud son sólo los que se encuentran en las instituciones y centros sanitarios públicos y privados y los tratados por los profesionales sanitarios, pues es éste el ámbito al que se refiere[596]. Sin embargo, es conocido que se pueden encontrar datos relativos a la salud en ficheros situados en otros lugares, como centros penitenciarios o escolares, o en empresas privadas. Hoy día, tras la aprobación del RDLOPD, el concepto de dato de carácter personal relacionado con la salud queda definido como “*las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética*”[597]. En el

[594] Anexo II Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud, BOPV nº 246, 28 de diciembre de 2006.
[595] MUNAR BERNAT, “El Tratamiento...”, 1997, p. 107.
[596] MARTÍN-CASALLO LÓPEZ, *Derechos de acceso...,* cit., 2000.
[597] Artículo 5.1g) RDLOPD.

ámbito sanitario la única referencia a esta cuestión se encuentra en la LBAP, que se refiere a la información clínica como "*todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla*"[598]. En el ámbito internacional la Memoria Explicativa del Convenio de 1981 entiende por dato relativo a la salud, la información referida a la salud pasada, presente o futura, física o mental de un individuo. La información puede referirse a una persona enferma, de buena salud o fallecida. Añade que esta categoría cubre también las informaciones relativas al abuso del alcohol o al consumo de drogas[599]. Por su parte, la Recomendación del Consejo de Europa que regula la protección de datos médicos se refiere a éstos como los "*datos personales relativos a la salud del individuo*", incluyendo "*los datos que tengan una clara y estrecha relación con la salud y los datos genéticos*"[600]. La Memoria Explicativa de esta Recomendación precisa que esa definición abraza la salud pasada, presente y futura, tanto la salud física como mental, y que recoge también cualquier información que tiene una relación directa con la situación sanitaria del individuo: el comportamiento del individuo, la vida sexual, el estilo de vida en general, el abuso de drogas, del alcohol y la nicotina. Se trata de información que tiene relación clara y directa con la salud[601].

Todas estas definiciones plantean fundamentalmente dos cuestiones. En primer lugar, se puede observar que cada una de las normas se refiere a objetos distintos: datos de salud, datos clínicos, datos médicos, y habrá que añadir, datos sanitarios. De inicio podría parecer que se trata de conceptos sinónimos. Lo cierto es que la utilización que en las normas se realiza de los mismos podría llevar a dicha conclusión, dado que se trata de términos que se emplean indistintamente. No obstante, es necesario, a pesar de que en la práctica se les otorgue un sentido similar, en aras de una mayor claridad, fijar el contenido exacto de cada concepto. Como se irá viendo, el concepto más genérico es el referente a los datos de salud, que engloba a todos los demás, que son datos de salud pero añadiendo algún matiz. En segundo lugar, por lo tanto, será obligatorio determinar el contenido y la amplitud del concepto datos de salud.

Estas dos cuestiones serán aclaradas en los apartados siguientes. En la medida en que se vaya determinando qué es lo que hay que entender por dato relativo a la salud se dará un contenido determinado a cada concepto citado. Sin embargo, merece la pena, por la importancia que tiene en este trabajo, llevar a cabo desde ahora la distinción entre dato de salud y dato sanitario.

La LOPD, y también el reglamento que la desarrolla, emplean el concepto de dato relativo a la salud cada vez que se hace referencia a la información que refleja cuál es el estado físico y mental de las personas. Sin embargo, en diferentes preceptos se prevé que este tipo de dato puede ser empleado en distintos sectores de la realidad. El artículo 7 de la Ley se refiere a esta información de manera general, es decir, a los datos de salud sea cual sea el ámbito en el que se manipulen: laboral, policial, etc. El artículo 8, por el contrario, regula la manipulación de esta

[598] Artículo 3 LBAP.
[599] Considerando 45 Memoria Explicativa del Convenio 108/1981 del Consejo de Europa.
[600] Artículo 1 R (97) 5.
[601] Considerandos 37 y 38 Memoria Explicativa de la Recomendación 5 (1997) del Consejo de Europa.

información en un ámbito específico. Se refiere en concreto al tratamiento de estos datos en las "instituciones y los centros sanitarios públicos o privados".

Si bien en ambos casos se trata de información que puede tener un mismo contenido, es necesario en aras de una mayor claridad distinguir ambos tipos de datos. Esto se debe al hecho de que el régimen jurídico a aplicar es, de inicio, distinto dependiendo de si la información es empleada con fines de proteger la salud de las personas o de otros fines. Evidentemente, en el ámbito que se regula en el segundo precepto la finalidad será, la mayoría de veces, la salvaguarda de la salud, mientras que en el ámbito regulado en el primero los fines pueden ser más variados. Partiendo de esta distinción se entenderá que cuando se utiliza el concepto "datos relativos a la salud" se está haciendo referencia a todos los datos relativos a la salud, independientemente del lugar en el que es tratada la información. Mientras tanto, se empleará el concepto de "dato sanitario" en un sentido más concreto, como el dato que se refiere a la salud de las personas, cuando es manipulado en el ámbito sanitario[602].

Se puede decir que el dato de carácter personal sanitario es dato de carácter personal relativo a la salud de las personas empleado en un sector determinado[603]. Es necesario, por lo tanto, delimitar el ámbito que abarca la información relativa a la salud.

V.2.2. En torno a la amplitud de la expresión "dato relativo a la salud".

De las definiciones que se han dado más arriba puede deducirse un concepto amplio de lo que ha de entenderse por dato de carácter personal relativo a la salud[604]. El RDLOPD al señalar que los datos de salud se refieren a la información concerniente a la salud cae en una redundancia que no aclara en exceso el contenido de dicho concepto. El único matiz que añade es que la información podrá referirse a la salud pasada, presente o futura. La LBAP, en referencia a la información clínica, parece aclarar algo más el contenido de este concepto. Al referirse a toda información, cualquiera que sea el formato en que aparezca, que concierna al estado físico o mental o a la forma de "*preservarla, cuidarla, mejorarla o recuperarla*", da un sentido más amplio de dicho concepto. Haciendo un simple ejercicio de interpretación es fácilmente deducible que los datos que se refieran a la forma de preservar, cuidar, mejorar o recuperar la salud de las personas pueden concernir a diferentes ámbitos de la vida: hábitos de consumo, ocio, vida sexual… Toda esta información podría catalogarse como información relativa a la salud de las personas. Parece, por lo tanto, que la acepción amplia de dicho concepto es la asumida en esta norma. Esta interpretación amplia encuentra su fundamento en el ámbito internacional. La memoria explicativa de la Recomendación del Consejo de Europa reconoce de manera expresa que se ha optado por la definición más amplia posible del dato médico[605]. En este mismo sentido, en el ámbito europeo los propios tribunales han otorgado un amplio alcance al concepto que ahora se analiza. En un

[602] MARTÍN-CASALLO LÓPEZ, *Derechos de acceso...,* cit., 2000; CONDE ORTIZ, *La Protección de Datos…,* cit., 2005, p. 73; ABEL LLUCH, "El derecho de información…", cit., 2004, p. 38, se refiere, en este sentido, a la información sanitaria como "aquélla relativa a lossistemas de salud del Estado o de una Comunidad Autónoma, sobre los servicios y unidades asistenciales disponibles y su forma de acceso"

[603] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 53, también lo define en este sentido.

[604] DE MIGUEL SÁNCHEZ, "Investigación y Protección…", cit., 2006, p. 150, apunta que la mayoría de la doctrina aboga también por este concepto amplio.

[605] Considerando 37 Memoria Explicativa Recomendación 5 (1997) del Consejo de Europa.

conocido caso concluyen los tribunales que la expresión datos relativos a la salud ha de entenderse en sentido amplio, llegando a interpretar que la indicación de que una persona se ha lesionado un pie y está de baja ha de incardinarse en dicho concepto[606].

En primera instancia, cabe destacar el hecho de que se recoja de forma expresa, en la definición de dato relativo a la salud, tanto la información concerniente a la salud presente como a la pasada y futura, tanto la referente a la persona sana como a la enferma o fallecida. Estas consideraciones no plantean mayores problemas de comprensión. Es evidente que toda esta información es necesaria para determinar cuál es la salud de las personas. No tendría sentido dejar a un lado, por ejemplo, los datos referentes al pasado o a los parámetros que determinan que una persona está sana, pues esta información es también necesaria para deducir la condición física y mental de cualquier sujeto en un momento determinado[607].

Los problemas comienzan cuando se trata de dar un contenido concreto al concepto de datos de salud y a determinar qué datos se incluyen en el mismo. En este sentido, en los distintos textos del Consejo de Europa, a los que se ha hecho referencia más arriba, se hace mención, más allá de a los datos estrictamente médicos, a las informaciones que sin ser en sentido estricto de salud afectan directamente a la misma. Como bien ha señalado la doctrina, se configura a la hora de interpretar la LOPD un concepto expansivo de dato de carácter personal relativo a la salud[608]. Desde un punto de vista práctico, si se tienen en cuenta todos los datos que los profesionales sanitarios tratan, se podrían distinguir tres esferas en base a su contenido.

A) En una primera esfera se podrían incluir los datos que indican exclusivamente el estado de salud de un individuo. Estos datos serán calificados aquí como "datos médicos"[609]. Las normas analizadas emplean indistintamente los términos "dato médico" y "dato relativo a la salud"[610]. Sin embargo, en favor de una mayor claridad se entiende que es posible distinguir los dos términos, considerando el dato relativo a la salud, que por otro lado es el que emplea la LOPD, como un concepto más amplio que el de dato médico. Así parece haberse interpretado en alguna ocasión por la doctrina[611] y también por grupos de trabajo que se han referido a esta cuestión[612].

[606] STJUE 6 noviembre de 2003, Bodil Lindqvist v. Aklagarkammanen i Jönköping, C-101/01.

[607] Resolución de la AEPD R/02635/2009, 9 de diciembre de 2009. Procedimiento PS/00325/2009, en el que se reconoce que incluso el dato de salud de carácter benigno es dato de salud. GÓMEZ RIVERO, *La Protección Penal*...,cit., 2007, p. 37

[608] RUBÍ NAVARRETE, "La autorregulación..*",* cit., 2003, p.387.

[609] En algún caso se han equiparado los datos médicos y los sanitarios, entendiéndolos como los datos de salud empleados en el ámbito sanitario. NICOLÁS JIMÉNEZ, "El Concepto de Dato…", cit., 2005, p. 79.

[610] Mientras que el Convenio 108/81 emplea el término "dato relativo a la salud", la Recomendación (97)5, emplea el de "dato médico".

[611] SÁNCHEZ CARO y ABELLÁN, *Derechos y Deberes*..., cit., 2003, p. 42, también parecen pronunciarse en este sentido al hacer suya la definición de DE LA CUEVA, quien entiende que "la expresión datos relativos a la salud (...) abarcaría tanto a los datos de carácter médico como aquellos otros que guarden relación con la salud".

[612] EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES, opinion nº 13, 30/07/1999, about *Ethical Issues of Healthcare on the Information Society.* http://.europa.eu.int/comm/european_group_ethics/avis_old_en.htm. "considera que la "información relativa a la salud" incluye, no sólo el básico dato médico: el historial de todos los diagnósticos médicos, enfermedades e intervenciones médicas, las medicaciones recetadas, los resultados de los distintos tests a los que se le ha sometido, incluyendo imágenes, etc.; sino que incorpora también el dato sensible relativo a la salud mental, las pautas de comportamiento, de

En relación a los datos que se refieren al estado mental se llegó a plantear en alguna ocasión la duda sobre la pertinencia o no de incorporarlos dentro del concepto citado. Lógicamente, la solución ha venido en forma afirmativa. En el ámbito internacional tanto el Convenio del Consejo de Europa como la Recomendación que regula la protección de datos médicos incorporan el dato psicológico al dato médico. En el ámbito estatal la AEPD[613] ha venido a aclarar esta cuestión manteniendo la misma línea interpretativa. Señala esta institución, fundamentándose en una recomendación del Consejo de Europa que se refería a esta cuestión[614], que no hay duda de que los datos psicológicos son datos relativos a la salud, independientemente de que estén recogidos en una HC o no[615]. La inclusión de este tipo de información en el concepto de datos relativos a la salud tiene fácil justificación. Como se verá, los datos de salud tienen una consideración especial en los diferentes textos legales y son objeto de una protección especial. Esto se debe a que el uso torticero de estos datos puede originar numerosos daños a los titulares de los mismos: piénsese las consecuencias que puede traer en el ámbito laboral o, incluso, social el que se dé a conocer que un sujeto es portador del VIH. Siendo esto así, parece descabellado admitir que los datos que se refieren a la salud mental de las personas no merecen la protección que se otorga en las normas a los datos de salud. La información sobre la condición psicológica de las personas, mal empleada, puede causar graves perjuicios a la persona titular de dichos datos. Piénsese, otra vez, por ejemplo en el ámbito laboral. La necesidad de que el concepto de dato de salud abrace también los datos concernientes a la salud mental resulta evidente.

En la primera esfera, en la que se hace referencia a los datos médicos, se recoge por lo tanto la información que estrictamente indica el estado de salud tanto física como mental de los individuos. Una interpretación restrictiva del concepto dato de salud podría llevar a entender que se limita a este tipo de información. Sin embargo, se entiende aquí que se ha de realizar una interpretación más amplia, que llegue a abrazar otros datos. Como se verá en el apartado siguiente, al analizar el principio de finalidad, el concepto "salud" se entiende en general en un sentido amplio abarcando no sólo lo estrictamente médico, sino todo aquello que afecta a la salud de las personas.

---

la vida sexual, los factores económicos y sociales, etc., y, también, los datos administrativos surgidos del cuidado médico: ingresos y altas, datos rutinarios de funcionamiento, de carácter económico, etc.".

[613] AEPD, *Informe jurídico de la APD sobre la naturaleza de los datos psicológicos a efectos de su tratamiento.* http://www.agpd.es/

[614] Recomendación 15 (1991) 11 de octubre de 1991, sobre Cooperación Europea en materia de Estudios Epidemiológicos en el Ámbito de la Salud Mental.

[615] La AEPD, con buen criterio, afirma que los datos psicológicos, aún no estando recogidos en una HC hay que considerarlos datos relativos a la salud. Hay que tener presente que cuando los datos psicológicos se encuentran en una HC será para que se dé un uso estrictamente médico de los mismos en un centro sanitario, mientras que cuando no se encuentran en una HC, será porque no están incorporados en dichos centros sino en otros lugares donde su uso no será el estrictamente médico sino cualquier otro, que probablemente conllevará para el titular de la información efectos mucho más perjudiciales. Por tanto, el no considerar esta información no contenida en la HC como relativa a la salud, supondría una clamorosa desprotección del individuo titular de la información relativa a su estado de salud mental ya que no se le aplicaría el régimen especial previsto en el art. 7 LOPD para los datos relativos a la salud. Incluso podría sugerirse que, en el ámbito estrictamente práctico, es más necesario aplicar el régimen especial al que nos hemos referido, a la información psicológica no contenida en la HC, que a la contenida en dicho documento, ya que al fin y al cabo, en el ámbito sanitario las garantías van a ser siempre mayores debido al fin último que se persigue en el mismo. Llama la atención, como habiendo aclarado la AEPD este punto, la Ley 41/2002 de 14 de noviembre, en la definición de "información clínica" se refiere exclusivamente al "estado físico", dando a entender que los datos relativos al estado de salud mental no se incorporan en dicha definición. SÁNCHEZ CARO y ABELLÁN, *Telemedicina y protección…*, cit., 2002, p. 45.

B) En la segunda esfera se encuentra la información que sin ser estrictamente médica guarda una estrecha relación con el estado de salud del individuo. La memoria explicativa del Convenio de 1981 hace una referencia puntual al "*abuso de alcohol y drogas*" incorporando esta información como relativa a la salud. La Recomendación relativa a la protección de datos médicos sigue la misma línea consolidando esa tendencia expansiva al emplear términos más genéricos que llegan a abrazar todos "*los datos que tengan una clara y estrecha relación con la salud*". Si bien la adjetivación "clara y estrecha" parece restringir el ámbito de aplicación, no se considera aquí que se puedan entender estos requisitos en términos restringidos. La propia memoria explicativa de la Recomendación afirma que la definición de dato de salud tiene que ser la más completa posible, y para ello, al establecer ejemplos de esa información de la que se puede deducir el estado de salud de un individuo, emplea conceptos tan generales como "*el comportamiento del individuo*" o "*el estilo de vida*" en general. En el ámbito interno la LBAP, aunque no hace una referencia expresa a este tipo de información, al incluir en el concepto de información clínica los datos sobre las acciones necesarias para preservar, cuidar, mejorar o recuperar la salud, parece adoptar el mismo criterio que las normas anteriores. En esta Ley el término de información clínica se estaría utilizando como sinónimo de dato relativo a la salud.

Resulta, por lo tanto, de estos textos una acepción amplia del concepto, incluyendo no sólo los datos estrictamente médicos, sino también los que sin serlo se refieren a aspectos de la vida que tienen incidencia en la salud[616]. Con esto no se quiere decir que este tipo de información constituye siempre dato relativo a la salud. Evidentemente, sólo será así cuando se emplee con la finalidad de proteger la salud de las personas[617]. Fuera del contexto sanitario estas informaciones difícilmente podrán considerarse datos de salud[618].

C) Junto a la información estrictamente médica y la que se acaba de considerar que forma una segunda esfera de datos de salud, hay que plantearse ahora si cabe hacer lo propio con los datos de carácter administrativo y económico que en los centros resultan del tratamiento sanitario. Se ha cuestionado si este tipo de información podría configurar una tercera esfera.

En los textos legales citados no se dice nada expresamente con respecto a este tipo de información. La doctrina, atendiendo al Derecho Comparado, ha puesto de manifiesto cómo hay normas que no reconocen los datos puramente administrativos o económicos como datos de salud y cómo, por el contrario, hay otros textos que sí lo hacen, caso de la Ley de Confidencialidad de los Datos Sanitarios estadounidense[619]. Desde el Consejo de Europa la

[616] SÁNCHEZ CARO y ABELLÁN, *Telemedicina y protección...*, cit., 2002, p.44, consideran que quedarían "comprendidos, por tanto, todos aquellos datos que tienen que ver con el cuerpo humano, como la sexualidad, la raza, el código genético, pero además, los antecedentes familiares, los hábitos de vida, de alimentación y consumo, así como las enfermedades actuales, pasadas o futuras previsibles, bien sean de tipo físico o psíquico; y las informaciones relativas al abuso de alcohol o al consumo de drogas (...). En definitiva, abarcaría todos los datos que de alguna forma se refieran a la salud tanto de individuos con buena salud, enfermos o fallecidos". Informe jurídico AEPD, 182/2004; MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, p. 32.

[617] Informe jurídico AEPD, 0129/2005, entiende que el dato de que una persona es fumadora no puede constituir un dato de salud, si no se asocia con algún indicador del efecto que este uso tiene sobre la salud del titular de la información.

[618] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 55.

[619] HEREDERO HIGUERAS, "La protección de datos…", cit., 1994, pp.19-20; SÁNCHEZ-CARO y ABELLÁN, *Datos de...*, cit., 2004, p. 17. En la citada norma (*Standards for privacy of individually identifiable health information),*

Recomendación que regulaba las bases de datos médicos, antes de la entrada en vigor de la Recomendación de 1997, extendía su ámbito de aplicación también a las informaciones sociales o administrativas[620]. También desde alguna agencia de protección de datos se ha admitido la consideración como dato de salud de, por ejemplo, el lugar de evacuación de una persona, debido a que dicha información se vinculaba con un expediente sanitario determinado[621].

Se entiende que el estado de salud de las personas puede desprenderse, aunque sea indirectamente, de indicadores de contenido administrativo o fiscal que están relacionados con tratamientos sanitarios determinados[622]. Parece, por lo tanto, conveniente que a este tipo de datos se les aplique el régimen jurídico que concierne a los datos de salud[623]. Para llevar a cabo la labor sanitaria se recogen informaciones que de inicio no indican nada sobre el estado de salud, pero que son necesarios para la gestión sanitaria, a saber: nombre y apellidos, domicilio, estado civil, etc. Se ha señalado por parte de la doctrina que este tipo de información no constituye estrictamente dato de salud pero que, al ser manipulado con la finalidad de proteger la salud de las personas queda afectado por dicho fin siendo sometido al régimen jurídico aplicable a los datos de salud[624]. Si bien es cierto que la mayoría de las veces este tipo de información de gestión administrativa y económica no refleja el estado de salud de las personas, no es menos cierto que esto no siempre es así. Piénsese en las referencias que se pueden realizar a números de historias clínicas en ficheros que tienen como fin el control de gastos económicos, en relación, por ejemplo, a la solicitud de material protésico[625]. Es evidente que si bien esta información tiene una finalidad puramente administrativa o de gestión, de ella pueden deducirse datos sobre la salud de las personas que aparecen en dichos ficheros. Sea como sea, parece necesario, aunque sólo sea por cuestiones prácticas, que a este tipo de datos se otorgue también la máxima protección[626], sobre todo porque en el ámbito sanitario, a pesar de que una información puede no considerarse estrictamente médica, la puesta en relación de dichos datos con otros conlleva que se tenga una visión más amplia de la salud de las personas[627].

---

que entró en vigor el 14 de abril de 2001, se definen los "datos relativos a la salud" como cualquier información, sea oral o grabada empleando cualquier forma o medio, que:
es creada o recibida por un proveedor de servicios de salud, plan de salud, autoridad pública de la salud, empresario, compañía de seguros de vida, escuela o universidad, o entidad encargada del tratamiento de datos de salud; y
se refiere a la salud o condición física o mental del pasado, presente o futuro de un individuo; a la provisión de cuidados de salud personales; o al pago de los servicios de salud que hubiera realzado una persona en el pasado, que se lleve a cabo en el presente o vaya a realizarse en el futuro.

[620] Artículo 1.2 del Anexo de la Recomendación 1 (81), del Comité de Ministros del Consejo de Europa, 23 de enero de 1981, que regula las bases de datos médicos automatizadas. MUNAR BERNAT, "El tratamiento...", cit., 1997, p. 109.

[621] Dictamen AVPD CN09-003, 5 de febrero de 2009.

[622] FREIXAS GUTIERREZ, *La protección...*, cit., 2001, p.146.

[623] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, pp. 176-177 también están de acuerdo en incorporar los datos administrativos y económicos que derivan del tratamiento dentro del concepto "dato relativo a la salud": "el que figure un paciente en el listado de la actividad económica de un centro sanitario (...) o que ha asistido a una consulta (...) significa que ese sujeto tiene o ha tenido algún problema de salud".

[624] SERRANO PÉREZ, *El Derecho...*, cit., 2003, p.411.

[625] Informe jurídico AEPD, 0625/2009.

[626] LARIOS RISCO, "La historia clínica…", cit., 2009, p.163, parece otorgar a toda la información contenida en la historia clínica, independientemente del contenido, la misma categoría.

[627] SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000, p. 112, señala que el que "un paciente figure en el listado de la actividad económica de un centro sanitario, simplemente señalando que ha tenido 5 o 6 estancias, o que ha asistido a una consulta (…) significa que ese sujeto tiene o ha tenido algún problema de salud".

V.3. El "dato relativo a la salud" como dato sensible.

La Ley realiza una clasificación entre distintos tipos de datos, estableciendo un régimen jurídico diferente según la categoría. Frente al régimen jurídico común, la Ley dispone una protección mayor para los datos relativos a la salud, el origen racial y la vida sexual. Para los datos que reflejen la ideología, afiliación sindical, religión y creencias se establece una protección aún mayor[628].

La importancia de fijar qué datos van a ser entendidos como datos relativos a la salud deriva del hecho de que a estos datos se les aplicará automáticamente por la LOPD el calificativo de "dato especialmente protegido" o, como se ha denominado en la doctrina[629] y también en la jurisprudencia[630], de "dato sensible", lo que supondrá que serán de partida objeto de una regulación más garantista.

Como se verá, las normas no definen con claridad un criterio concreto para justificar el porqué de la consideración de unos datos como sensibles. Es por ello por lo que en las siguientes líneas se tratará de aportar, partiendo de los textos normativos, unos parámetros que sirvan para identificar dichos datos en la práctica.

---

[628] Artículo 7 LOPD: -*Datos especialmente protegidos- 1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.*
Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".

[629] MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 273; GUICHOT, *Datos Personales…,* cit., 2005, p. 218; GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 74.

[630] SSTS 15 de noviembre de 2004, FJ 9, que se refiere a los datos relativos al consumo de drogas, vinculados a los datos de salud, como datos sensibles debido a que "pueden provocar un juicio de valor social de reproche o desvalorización ante la comunidad"; 30 de diciembre de 2009, FJ, 11, en el que se refiere a los datos sanitarios como datos sensibles. SAN 7 de junio de 2006, FJ, 5, en el que argumenta que al tratarse de datos no sensibles la infracción ha de ser menor. STEDH 4 de diciembre de 2008, caso S y Marper c. Reino Unido, FJ 203, hace referencia a los datos de ADN como datos sensibles en la medida en que de ellos se desprende numerosa información sobre un sujeto y su familia.

V.3.1.El contexto como criterio para determinar la sensibilidad de la información.

Los criterios a la hora de determinar que unos datos han de ser considerados sensibles pueden ser distintos. Si se hace un primer acercamiento a las distintas normas que se han citado, se observará que realizan una clasificación entre distintos tipos de datos, considerando unos de ellos como merecedores de una mayor protección que la normal[631]. La Directiva europea expresamente hace referencia a la naturaleza de los datos como argumento que justifica una tal clasificación[632]. Partiendo de estas previsiones algunos autores parecen entender que una información tiene el carácter de sensible cuando afecta a la esfera más íntima del individuo[633]. Se trataría de una información que toca el ámbito más interno de las personas[634]. Se acepta por este grupo de autores que es la naturaleza de esos datos la que determina la sensibilidad de los mismos[635]. En algún caso la jurisprudencia del TEDH parece haber seguido esta posición[636]. También en el ámbito interno la jurisprudencia ha mantenido en alguna ocasión esta postura[637], si bien pueden encontrarse supuestos en que se matiza con mayor profundidad en esta cuestión para abrir la puerta a nuevos argumentos[638].

Siguiendo esta línea interpretativa la conclusión llevaría a la distinción entre unos datos que por su naturaleza afectan de forma especial a la intimidad de los individuos, y que resultarían merecedores de una protección mayor, y otros datos que al no tener esa naturaleza cualificada no serían objeto de esa especial protección. Así pues, el nivel de protección se establecería atendiendo a la naturaleza de los datos.

Cabe preguntarse si es realmente posible realizar tal distinción, en términos tan absolutos, y si eso es a su vez práctico. El mayor problema que se plantea al tratar de seguir esa teoría es el de fijar una lista de datos objetivamente íntimos. ¿Cuáles son esos datos íntimos que afectan a lo más profundo del ser? Quizá no sea totalmente descabellado asumir la existencia de unos datos que en un momento histórico concreto puedan ser aceptados por la "razón social" como merecedores de una protección especial. Pero de ahí a configurar, como parece hacer la LOPD,

631 Ya se ha citado el artículo 7 de la LOPD. El artículo 8 Directiva 95/46/CE recoge, prácticamente, el mismo tipo de datos como los merecedores una protección especial.

632 Considerando 33 Directiva 95/46/CE: "*(...) los datos que por su naturaleza puedan atentar contra las libertades fundamentales o la intimidad no deben ser objeto de tratamiento alguno (...)*".

633 FERNÁNDEZ LÓPEZ, "El Derecho...", cit., 2003, p. 42; CONDE ORTIZ, *La Protección de Datos…,* cit., 2005, p. 69; MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, p. 29; GÓMEZ SÁNCHEZ, "Datos de salud…", cit., 2010, p. 648: "Los denominados datos de salud deben recibir una protección reforzada en todo caso en razón de la información que revelan o pueden llegar a revelar y no en función del fin objeto del tratamiento de dichos datos".

634 DEL PESO NAVARRO, *Qué pasa...,* cit., http://www.iee.es/.

635 RIPOL CARULLA, "La Protección...", cit., 1996, p.119; RIPOL CARULLA, *El Tratamiento...*, cit., 1999, p. 145, considera que "por la naturaleza de la información a la que se refieren, los datos médicos y genéticos forman parte de la esfera más íntima de las personas".

636 SSTEDH 26 marzo de 1987, Leander y 5 mayo del 2000, caso Rotaru.

637 STC 23 marzo de 2009, FJ 2, en el que el Tribunal admite que los datos de salud son merecedores de una mayor protección debido a que afectan a la intimidad de las personas.

638 STS 15 de noviembre de 2004, FJ 9, que se refiere a los datos relativos al consumo de drogas, vinculados a los datos de salud, como datos sensibles debido a que "pueden provocar un juicio de valor social de reproche o desvalorización ante la comunidad"

una lista cerrada de datos sensibles, íntimos *per se*, como si fuera un elemento estático, hay mucha diferencia.

Y si problemático parece establecer esa lista de datos que por sí mismos se constituyen en sensibles, más problemática parece la postura adoptada por la LOPD, que no sólo se decanta por aceptar la existencia de unos datos especialmente protegidos o sensibles *per se*, sino que además hace una distinción en tres grupos de estos datos. Por un lado están los datos que revelan la ideología, afiliación sindical, religión y creencias, a los que se les da una protección máxima; por otro los relativos al origen racial, a la salud y a la vida sexual, que se protegen de manera especial, pero sin llegar al extremo del grupo anterior; y por último, los relativos a la comisión de infracciones penales o administrativas, que también se sujetan a un régimen especial. Si, como se comentaba, era difícil justificar la inclusión en la norma de una lista cerrada de datos sensibles, más difícil resulta argumentar el porqué a la información contenida en el artículo 7.2 de la LOPD se le otorga una mayor protección que a la contenida en el artículo 7.3 de la Ley. ¿Cuál puede constituir el argumento para proteger con mayor vigor que a los datos relativos a la vida sexual[639], los datos relativos a la afiliación sindical?[640] Según algún autor la distinción se produce en atención a lo que dispone el artículo 16.2 CE, que se refiere a la imposibilidad de obligar a nadie a declarar sobre su ideología, religión o creencias[641]. Se trata de la justificación que daba la LORTAD en su Exposición de motivos[642] y que se mantiene en principio en la LOPD, que hace mención expresa a esta disposición de la CE, pero que, según la misma corriente doctrinal, ha desmontado la propia Ley al incluir la "afiliación sindical", que no se recoge en el citado precepto constitucional, en dicho grupo de datos hipersensibles[643].

La fijación de distintas categorías de protección atendiendo a la naturaleza de los datos parece imposible, porque no es factible establecer un criterio material objetivo con fundamento alguno para realizar esa distinción. En el fondo, atender a la naturaleza, como se ha tratado por algunos sectores, para determinar el nivel de protección de los datos de carácter personal atentaría contra la propia base del derecho a la autodeterminación informativa, que tiene su fundamento en la conocida sentencia del Tribunal Constitucional Federal Alemán de 15 de diciembre de 1983[644], que precisamente parte de la consideración de que todos los datos son relevantes, y que incluso el que *a priori* puede parecer más inocuo puede convertirse, dependiendo del uso que se le dé, en reflejo del perfil de un individuo. Por un lado, la valoración de lo que es íntimo y no lo es ha ido cambiando a lo largo del tiempo e inevitablemente lo seguirá

[639] Incluso el propio TC ha admitido que los datos relativos a la vida sexual pertenecen a uno de los "reductos más sagrados" de la intimidad. STC 3 de junio de 1987 FJ 2.
[640] FREIXAS GUTIERREZ, *La protección...*, cit., 2001, p.130.
[641] SERRANO PÉREZ, *El Derecho...*, cit., 2003, p. 390.
[642] Exposición de motivos LORTAD: "*(...) se refuerzan singularmente en los denominados "datos sensibles" (...), de una parte, la ideología o creencias religiosas –cuya privacidad está expresamente garantizada por la Consitutción en su artículo 16.2- y de otra parte, la raza, la salud y la vida sexual*".
[643] ALONSO MARTÍNEZ, "Aproximación a Determinados...", cit., 2000, p. 10. La inclusión de la "afiliación sindical" en este grupo ha sido criticada por DAVARA RODRÍGUEZ y ALONSO MARTÍNEZ, quienes afirman que "los datos relativos a la afiliación sindical de una persona no tienen por qué revelar su ideología que, incluso pudiera ser contraria o diferente a la del sindicato al que pertenece".
[644] Puede leerse esta fundamental sentencia en el *BJC* nº33, enero de 1984, p. 126. Un interesante comentario a la citada sentencia se encuentra en HEREDERO HIGUERAS, "La Sentencia...", cit., 1983.

haciendo[645]. Por otro, la intimidad es una esfera subjetiva que cada individuo la delimita a su manera: lo que para una persona es íntimo puede no serlo para los demás[646]. Lo íntimo está sujeto a valoraciones subjetivas, individuales y colectivas, lo que imposibilita que pueda establecerse una lista cerrada de datos sensibles que afectan de forma particular a la intimidad y que, por lo tanto, son merecedores de una especial protección[647].

El criterio a seguir para determinar si un dato es o no sensible, y fijar así el nivel de protección, tiene que ser otro, distinto al que emplea la LOPD, que parece fundamentarse en el supuesto acercamiento de los datos que son objeto de especial protección a la esfera estrictamente íntima del individuo. Tiene que tratarse de un criterio más dinámico, flexible y abierto[648].

Siguiendo una corriente doctrinal distinta a la expuesta hasta ahora, se entiende que la sensibilidad se debe otorgar a los datos atendiendo al uso que se vaya a dar a los mismos y no a su naturaleza[649]. Efectivamente, dependiendo de la finalidad con que se manipule la información variará el nivel de protección que se haya de dar a la misma. Dependiendo, por lo tanto, del caso concreto unos datos pueden ser considerados sensibles o no[650]. Los datos no son sensibles según su naturaleza, sino que lo serán según las circunstancias en que se empleen.

Este criterio, que en un principio parece que no tiene aplicación o cabida en la LOPD, puede resultar de una lectura sistemática de la propia Ley. Es claro que de inicio la Ley atiende a la naturaleza de la información para realizar la clasificación a la que antes se ha hecho referencia. Sin embargo, si se observa su articulado desde una perspectiva general, se verá que incluso la propia LOPD acaba atendiendo, aunque sea inconscientemente, al uso que se vaya a dar a la información, al contexto en el que se va a realizar dicho uso, para determinar si unos datos se han de someter a un régimen especial o no. Esta circunstancia se da, concretamente, cuando regula el tratamiento de los datos de salud. Así, si bien en el artículo 7.3 establece que los datos relativos a la salud son datos especialmente protegidos, se entiende que por su naturaleza, en el artículo 8 el nivel de protección se rebaja cuando los datos relativos a la salud son tratados por profesionales sanitarios. Efectivamente, dependiendo de la finalidad con que se usen los datos, de quien los use, en definitiva, del contexto en que se manipulen, el régimen variará, porque el

[645] SERRANO PEREZ, *El Derecho...*, cit., 2003, p. 379: "Las distintas sociedades, en cada momento histórico, extienden la idea de reservar y mantener una determinada forma de vida, es decir, reducen o amplían las facetas de la vida que son menos públicas, o bien aceptan unos comportamientos y censuran otros (...) esto es, hoy por hoy la raza es una información protegida, pero en el camino hacia la globalización quizá deje de ser lo extraordinario para convertirse en habitual y con ello en no significativo, de cara a una protección especial".

[646] Exposición de Motivos Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen: "*se estima razonable admitir que (...) la esfera del honor, la intimidad personal y familiar y del uso de la imagen está determinada de manera decisiva por las ideas que prevalezcan en cada momento a la Sociedad y por el propio concepto que cada persona según sus actos propios mantenga al respecto y determine sus pautas de comportamientos*".

[647] MESSÍA de la CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 273.

[648] SÁNCHEZ BRAVO, La Regulación..., cit., 1994, p. 121. "La tutela de las informaciones no puede ya quedar limitada a aquellas de cuya calidad así se exija, en una visión estática, sino que debe extenderse a la dinámica de su uso o funcionalidad". MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 274; NICOLÁS JIMIÉNEZ, *La Protección Jurídica…,* cit., 2006, p. 75.

[649] SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000, p. 51; MESSÍA de la CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 274. GÓMEZ RIVERO, *La Protección Penal…*,cit., 2007, pp. 36-37.

[650] HEREDERO HIGUERAS, "Ante la Ratificación...", cit., 1983, p. 757.

riesgo para que se pueda llevar a cabo un uso que genere consecuencias perjudiciales para el titular también varía[651].

Evidentemente, no es lo mismo que los datos relativos a la salud se utilicen en el sector sanitario, donde se emplean con la finalidad de salvaguardar la salud de la ciudadanía, por lo que el uso de la información deberá ser más continuo, dinámico, flexibilizándose la normativa; o que se manipulen en una empresa aseguradora donde la finalidad puede ser discriminatoria (que no se conceda un seguro a personas con determinadas enfermedades es sólo un ejemplo), por lo que la normativa tiene que ser, necesariamente, más garantista. Si bien en casos limitados, esta posición también ha tenido eco en alguna ocasión en la jurisprudencia, aceptando que determinados datos que no son *a priori* sensibles pueden llegar a tener esa consideración[652].

En definitiva, se puede afirmar que dependiendo del contexto un dato en principio irrelevante puede constituirse en verdaderamente importante[653], y un dato que en principio es de máxima sensibilidad puede ser tratado de una forma más flexible, rebajando en cierta medida las garantías[654]. El contexto afecta a los datos que en él se traten y hace que, mediante esa afección, se les aplique un régimen distinto que el que de partida se tenía previsto se les aplicase.

V.3.2.La consideración de determinados datos como sensibles *a priori.*

Se ha asumido que todos los datos, por irrelevantes que en un principio puedan parecer, pueden convertirse en sensibles dependiendo del contexto. Sin embargo, a pesar de este planteamiento, no se puede negar la existencia de informaciones que de partida merecen un régimen de protección especial, no por su supuesta proximidad a la esfera más íntima del individuo, sino porque debido a su contenido un uso inadecuado de dicha información constituye un riesgo de envergadura para que se den consecuencias perjudiciales para el titular, sobre todo de carácter discriminatorio.

Se trata de informaciones que en el actual contexto han adquirido una relevancia social especial y que, por lo tanto, necesitan, *a priori,* una protección mayor que los demás datos. Esta

[651] RIPOL CARULLA, "El tratamiento...", cit., 1996, ha criticado duramente la dualidad de regímenes de la LORTAD (hoy vigente en la LOPD), al entender que tiene que ser la naturaleza del dato el determinante del nivel de protección y no el contexto. Afirma este autor que la "categoría de *datos sensibles* o especialmente protegibles (...) supone rechazar, como ya se ha dicho, la idea de que la información sobre una persona es neutra y que, por tanto, los peligros que de ella se deriven sólo pueden provenir del contexto en que se use".

[652] STS 15 de noviembre de 2004, FJ 9, que se refiere a los datos relativos al consumo de drogas, vinculados a los datos de salud, como datos sensibles debido a que "pueden provocar un juicio de valor social de reproche o desvalorización ante la comunidad"

[653] SÁNCHEZ BRAVO, *La regulación...*, cit., 1994, p. 122. "Existe la posibilidad (...) que datos *a priori* irrelevantes desde la consideración de la privacidad de las personas, sin embargo, en conexión con otros datos puedan servir para hacer completamente diáfana y transparente la personalidad de los ciudadanos". En el mismo sentido SIMITIS en el estudio *Revisiting Sensitive data,*1999, http://www.coe.int/ realiza la siguiente afirmación:"*sensitivity is no more perceived as an a priori given attribute. On the contrary, any personal datum can, depending on the purpouse or the circumstances of the processing be sensitive (...). The specific interests of the controller as well as of the potential recipients of the data, the aims for which the data are collected, the conditions of the processing and its posible consequences for the person concerned are factors that, put together, allow both the range and the effects of the of the processing to be discerned and thus to determine its degree of sensitivity*".

[654] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, p. 98.

previsión ha sido aceptada también en algún caso por la doctrina[655]. Es más, la memoria explicativa del Convenio del Consejo de Europa de 1981 reconoce que "*si bien el riesgo que para las personas supone el tratamiento de los datos, depende no del contenido sino del contexto en que se usan, hay casos excepcionales en los que el tratamiento de ciertos datos puede causar, como tal, daños a los derechos e intereses de los individuos*"[656].

A la hora de determinar qué datos son los que han de estar sometidos de partida a un régimen de protección especial habrá que atender no al artículo 16 de la CE, sino a su artículo 14[657]. Es este precepto el que constituye la base para determinar qué datos son los que *a priori* hay que proteger con mayor vigor. Por un lado, porque plantea el "riesgo de discriminación" como factor fundamental para determinar que a un dato haya que aplicarle un régimen más garantista[658], y no la mayor cercanía a la esfera más interna del individuo; y por otro lado, porque se trata de una cláusula abierta que permite incluir otros datos en este grupo[659].

Partiendo de lo dicho hasta ahora hay quien ha tratado de realizar una catalogación de los datos en distintos grupos. Los datos podrían dividirse en "indiferentes", caso, por ejemplo, del nombre, edad o fecha de nacimiento; "sensibles atendiendo al contexto en que se traten", entre los que se incluyen los clínicos; y "sensibles por sí mismos", como las opiniones políticas, creencias, vida sexual, origen racial[660]. Esta misma clasificación parece haberse realizado en algún caso en relación a los datos de salud, distinguiendo entre datos de salud que afectan de manera especial a los derechos de las personas y datos de salud que no afectan de esa forma a dichos derechos[661]. Se sobrentiende aquí que dicha clasificación conllevaría la aplicación de regímenes jurídicos distintos a cada grupo, otorgando mayor o menor protección dependiendo del caso.

Se puede estar de acuerdo en la idea de realizar una clasificación previa de las informaciones tomando en cuenta el riesgo que, *a priori*, puede suponer un uso irregular de las mismas para el ejercicio de derechos y libertades. Sin embargo, esta clasificación habrá que entenderla no como un esquema estático sino dinámico, donde los grupos se comunican dependiendo del uso que se dé a las informaciones que los integran. Al margen de la crítica que se pueda hacer a la inclusión de unos u otros datos en los distintos grupos[662], lo cierto es que, atendiendo al riesgo inherente en

[655] SERRANO PÉREZ, *El Derecho...*, cit., 2003, p. 379.
[656] Considerando 43 Memoria Explicativa Convenio 108/1981 del Consejo de Europa.
[657] Artículo 14 CE: "*Los españoles son iguales ante la ley, sin que pueda prevalecer discriminación alguna por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social"*. MESSÍA DE LA CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 277; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, pp. 107-108, no se muestra de acuerdo con esta consideración.
[658] VELÁZQUEZ BAUTISTA, *100 Interrogantes…*, cit., 2004, p. 24; GUERRERO PICÓ, *El Impacto de Internet…*, cit., 2006, p. 267.
[659] SEOANE RODRÍGUEZ, "De la Intimidad...", cit., 2002, p. 96, considera que "el aumento notable del riesgo de infracción y lesión de tales derechos mediante un uso inadecuado de los datos de carácter personal; y el carácter de contexto básico para el ejercicio de la libertad y el libre desarrollo de la personalidad del principio de igualdad", hacen que se tenga que tomar como referencia el artículo 14 de la CE en vez de el 16 CE para la determinación de los datos sensibles.
[660] VELÁZQUEZ BAUTISTA, *Protección Jurídica...,* cit., 1993, p. 379.
[661] NICOLÁS JIMÉNEZ, *La Protección Jurídica...,* cit., 2006, pp. 74-75.
[662] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos*..., cit., 1999, pp. 91.92: "Los datos que introduce en cada uno de los grupos son muy discutibles. Así, él defiende que la fecha de nacimiento es un dato

el contenido de los datos que forman cada grupo, es aceptable que se distingan diferentes grupos de informaciones. Sin embargo, ello no puede suponer que la información contenida en un grupo no pueda ser tratada, en un contexto determinado, aplicándose un régimen correspondiente a otro grupo de datos. Los datos relativos al origen racial de las personas, por ejemplo, que serían objeto, *a priori*, de una alta protección, pueden verse sometidos en determinados contextos a un régimen de salvaguarda más laxo. A nadie se le escapa que este tipo de datos son manipulados, más hoy en día, en el ámbito policial atendiendo a un régimen jurídico en el que muchos de los derechos que componen el derecho fundamental a la autodeterminación informativa, caso del derecho a consentir o ser informado, son exceptuados.

Después de todo lo dicho hay que valorar brevemente la inclusión de los datos de salud en el precepto dedicado en la Ley a los datos objeto de una protección especial. Más allá de que no se entienda la distinción que se hace en la Ley de estos datos respecto a los datos relativos a la ideología, religión, afiliación sindical y creencias, la consideración de los datos relativos a la salud como datos sensibles hay que valorarla como acertada. Esta conclusión se debe a que se trata de una información que por su contenido si es empleada de manera torticera puede causar graves perjuicios a su titular. Es más, siguiendo este criterio, puede llegar a entenderse que dentro de los propios datos de salud no toda la información tiene la misma relevancia a la hora de aplicar la Ley. Evidentemente, no es lo mismo que un dato refleje que el estado de salud de un sujeto es satisfactorio, a que se refiera a la infección por VIH de una persona[663]. El perjuicio que se puede causar a una persona mediante el uso irregular de esta última información es mucho mayor que el que se pueda causar empleando la primera. Esta conclusión, a pesar de no estar prevista en la LOPD, se recoge también en la jurisprudencia. Los tribunales han atendido al contenido concreto de los datos de salud que se pretenden manipular, si se refieren a una enfermedad con connotaciones especiales como el Sida, a la hora de ponderar si su uso en un contexto determinado ha sido acorde a Derecho o no[664].

La consideración positiva de la Ley, sin embargo, no resultaría tan positiva si la referencia a los datos de salud se acabara en su inclusión en la categoría de sensible, pues de dicha interpretación podría resultar la aplicación de un régimen jurídico único especialmente garantista. La valoración positiva de la inclusión de los datos de salud en el artículo 7 de la LOPD viene justificada porque paralelamente a lo dispuesto en dicho precepto, tanto el propio artículo 7 en su apartado sexto como el articulo 8 de la Ley plantean la posibilidad de que esta misma información, cuando se convierte en sanitaria al ser tratada en centros sanitarios, o cuando es manipulada con la finalidad de proteger la salud de los ciudadanos, pueda ser empleada de forma más flexible. Se prevé por lo tanto, en el caso de los datos relativos a la salud un régimen suficientemente flexible como para que se acomode a los distintos contextos en los que pueden ser tratados.

indiferente, cuando según el contexto en que se trate dicha información, puede hacer que se convierta en muy sensible, por ejemplo en ambientes laborales o para temas de salud, pues no hay que olvidar que el pronóstico y tratamiento de muchas enfermedades va a depender de la edad del sujeto. No menos discutible resulta la opción de agrupar los datos de salud entre los datos sensibles según el contexto en que se traten".

[663] Resolución de la AEPD R/00342/2008, 14 de abril de 2008. Procedimiento PS/00059/2008.

[664] SAN 16 de enero de 2008, FJ 3.

Evidentemente, en esos contextos determinados será necesaria una normativa suficiente que regule el tratamiento de los datos relativos a la salud[665].

[665] SERRANO PÉREZ, *El Derecho...*, cit., 2003, p. 414, resuelve el problema interpretativo que plantea la convivencia de los artículos 7 y 8 de la LOPD diciendo, en línea con lo expuesto, que el "uso de los datos en el terreno sanitario se regula en el artículo 8, que prevé un régimen particular para ellos en atención a su calificativo de especialmente delicados, mientras que el artículo 7º contempla la vida de estos fuera de aquél. En ambos casos se trata del mismo tipo de datos cuyo calificativo recoge el artículo 7 pero en el artículo 8 se hace depender su régimen de su finalidad asistencial".

CAPÍTULO 3. LOS PRINCIPIOS QUE DETERMINAN LA CALIDAD DE LOS DATOS.

Uno de los pilares en los que se fundamenta toda manipulación de datos de carácter personal lo constituyen los llamados "principios generales o básicos que afectan a la calidad de los datos", que son los que se recogen en el artículo 4 de la LOPD.

I. DEFINICIÓN Y DISTINCIÓN DE LOS PRINCIPIOS QUE DETERMINAN LA CALIDAD DE LOS DATOS. APROXIMACIÓN A LOS PRINCIPIOS DE FINALIDAD, PERTINENCIA Y VERACIDAD.

La hoy vigente Ley Orgánica de protección de datos y el reglamento que la desarrolla se refieren a dichos principios como principios relativos a la "calidad de los datos". Así lo hacen también la Directiva[666] y el Convenio del Consejo de Europa[667] que regulan esta materia. Estas normas no aclaran el significado de este enunciado. Sin embargo, su posición preferente en sus articulados da una idea de la importancia que se otorga a los mismos.

Para encontrar una aclaración al respecto hay que acudir a la ya derogada LORTAD. Esta Ley se refería a estos principios como los "principios generales de la protección de datos". La jurisprudencia se refiere a los principios generales del derecho como la "atmósfera en que se desarrolla la vida jurídica, el oxígeno que respiran las normas"[668]. Se trata de principios que dan coherencia y sentido al conjunto de normas que conforman un ordenamiento[669]. De esta manera, al referirse la LORTAD a los principios de calidad como principios generales, parecía reflejar la idea de que estos criterios constituyen la columna vertebral del marco en el que se ha de desenvolver todo tratamiento de datos. Se asume que se trata de fuentes que se encuentran en el fundamento mismo del ordenamiento dirigido a regular esta materia. Esta consideración se reforzaba en dicha Ley cuando aclaraba que estos principios "*definen las pautas a las que debe atenerse la recogida de datos de carácter personal*"[670].

La jurisprudencia también se ha acercado en alguna ocasión a definir estos principios. Siguiendo la aclaración de la LORTAD se ha entendido que son "las pautas a las que debe atenerse la recogida, tratamiento y uso de los datos de carácter personal"[671]. Queda clara aquí también la intención de comprender estos principios como auténticos principios generales que deben guiar toda manipulación de datos.

Atendiendo al marco normativo y jurisprudencial que se ha expuesto se podría concluir que la LOPD, cuando regula los principios que determinan la "calidad de los datos", se refiere a los principales criterios que tiene que seguir todo tratamiento de datos de carácter personal. Parece, por lo tanto, que el contenido de estos preceptos se refiere a auténticos principios básicos de la protección de datos. Mientras otras figuras que también son consideradas en la Ley como principios y que más adelante se analizarán, como el derecho a consentir una manipulación de

[666] Artículos 5 y 6 Directiva 95/46/CE, 24 de octubre de 1995.
[667] Artículos 4 y 5 Convenio 108/1981 del Consejo de Europa.
[668] SSTS 27 de julio de 1987, FJ 1 y 27 de mayo de 1998, FJ 6.
[669] LASAGABASTER HERRARTE, *Fuentes del Derecho…,* cit., 2007, pp. 246-247.
[670] Exposición de Motivos LORTAD.
[671] SAN de 24 de marzo de 2004, FJ 2.

datos o el derecho a ser informado sobre las características que rodearán un tratamiento concreto, pueden encontrarse con excepciones en su aplicación, los principios que determinan la calidad de un tratamiento difícilmente pueden encontrar límites. Toda operación de manipulación de datos de carácter personal los ha de tener en consideración.

Su importancia se reconoce en la actualidad en todas las normas que regulan la protección de datos de carácter personal. Como se irá viendo, en todas se erigen como los principales criterios a tener en cuenta para determinar si un tratamiento de datos es acorde a Derecho o no.

Como ha expuesto la doctrina, del contenido del artículo 4 de la LOPD pueden distinguirse diferentes principios básicos. De una primera lectura se podría extraer la conclusión de que son tres los que en todo momento tienen que inspirar el tratamiento. Por un lado habría que señalar el principio de "finalidad" que determina que *"los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos*"[672]. Por otro al que se ha denominado principio de "pertinencia". Éste lleva a la idea de que "*los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido*"[673]. Y, por último, se encuentra el principio de "veracidad", según el cual "*los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado*"[674].

Los tres principios indicados tienen autonomía propia y responden a unas exigencias determinadas. Sin embargo, se entiende en última instancia que todos los principios giran en torno al de finalidad, que es sin duda alguna el fundamental del marco jurídico regulador de la protección de datos de carácter personal[675]. El principio de pertinencia está íntimamente ligado al de finalidad en la medida en que el grado de pertinencia en el tratamiento de los datos de carácter personal se mide tomando como referencia la finalidad para la que los datos son manipulados: los datos son pertinentes o no, para el cumplimiento de una finalidad determinada[676]. La relación entre el principio de veracidad y el de finalidad es también clara. Para que los datos cumplan con el fin para el cual fueron recogidos es absolutamente necesario que estos datos estén actualizados y que respondan siempre a la realidad, pues no tiene sentido alguno que se empleen datos de carácter personal con un fin determinado si éstos son erróneos[677].

La inclusión de esos principios en las normas que regulan el derecho a la autodeterminación informativa ha sido generalizada. Tanto en el ámbito estatal como en el internacional cuando se

[672] Artículo 4.2 LOPD.
[673] Artículo 4.1 LOPD.
[674] Artículo 4.3 LOPD.
[675] FERNÁNDEZ SALMERÓN, *La Protección de los datos…*, cit., 2003, p. 95, también subraya el hecho de que el principio de finalidad constituye el criterio vertebrador sobre el que giran los demás principios.
[676] GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 78.
[677] HEREDERO HIGUERAS, *La Directiva*..., cit., 1997, p. 103; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 409.

hace referencia a los principios se reconocen los citados. La regulación en todos los ordenamientos es además muy similar, empleando fórmulas parecidas. Sin embargo, hay pequeñas diferencias que hay que tener en cuenta. A la hora de interpretar la regulación que la LOPD hace de estos principios habrá que tomar en consideración lo que establecen no sólo la citada Ley, sino también, fundamentalmente, la LORTAD, la Directiva 95/46/CE y el Convenio de 1981, sin olvidar lo que la jurisprudencia y los diferentes autores han señalado al respecto.

II. EL PRINCIPIO DE FINALIDAD EN EL TRATAMIENTO DE DATOS DIRIGIDO A PROTEGER LA SALUD DE LAS PERSONAS.

El análisis del principio de finalidad en la manipulación de los datos de carácter personal, en el ámbito específico de la Administración sanitaria, exige el estudio y la interpretación de dicho principio desde diferentes perspectivas. En primer lugar, desde un punto de vista general, atendiendo a los postulados que marca la normativa reguladora de la protección de datos. Y en segundo lugar, desde una perspectiva más concreta, analizando la normativa que regula la actividad sanitaria. Interesa en este sentido aclarar a qué se hace referencia cuando se señala que los datos podrán ser manipulados con el fin de "proteger la salud de las personas".

II.1. La finalidad en la normativa reguladora de la protección de datos de carácter personal.

Es necesario acudir a distintas normas para poder determinar las características de la finalidad desde la perspectiva de la protección de datos de carácter personal. El artículo 4.2 de la vigente LOPD ya se ha trascrito. El mismo artículo de la anterior LORTAD disponía que "*los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos"*. El artículo 6.1.b) de la Directiva 95/46 señala que "*los Estados miembros dispondrán que los datos personales sean: b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas".* Ya se ha comentado al inicio de este capítulo, que de una primera lectura de estos artículos es posible deducir que el tratamiento de este principio por parte de estas normas ha sido bastante similar. Sin embargo, un análisis exhaustivo de estos preceptos hará ver que existen pequeñas diferencias entre las mismas que deben ser tenidas en cuenta.

II.1.1. Definición y relevancia del principio de finalidad.

Las normas arriba citadas no entran a definir este principio. No obstante, puede entenderse que cuando en la LOPD se hace referencia a la finalidad se está hablando de los objetivos que se persiguen con la manipulación de los datos, al por qué concreto del tratamiento[678]. En definitiva, la finalidad se refiere a los motivos en que se fundamenta la utilización de los datos por

[678] http://rae.es/: La RAE define el concepto "fin" como el "objeto o motivo con que se ejecuta algo".

parte del que será el responsable del fichero, a la actividad a la que dirige dicho responsable la manipulación de la información[679].

Al principio de finalidad se le ha otorgado un papel especialmente relevante en las normas que regulan la protección de datos de carácter personal. Así lo ha interpretado la doctrina[680]. Es cierto que todos los principios que componen el apartado concerniente a la calidad de los datos son tratados como principios fundamentales. Sin embargo, tanto la LOPD como la LORTAD y la Directiva europea basan gran parte de la regulación del derecho a la autodeterminación informativa en el principio de finalidad. En la mayoría de las facultades que componen este derecho y en los criterios que determinan la validez de los tratamientos este principio tiene una presencia importante.

En la regulación del derecho a ser informado ya se fija la necesidad de informar sobre la finalidad de la recogida de los datos[681]. A la hora de determinar cómo ha de llevarse a cabo la cesión de datos la finalidad adquiere también un protagonismo indiscutible. La cesión de los datos sólo será posible en la medida en que se dirija al cumplimiento de determinados fines[682]. Pero es sobre todo en relación con el consentimiento donde el principio de finalidad adquiere una relevancia especialmente significativa. Primero, porque la capacidad de control que el titular de los datos tiene sobre éstos, es decir, la autodeterminación informativa, ha de comenzar con el conocimiento por éste del fin al que se va a dirigir el tratamiento de los datos. El titular dará su autorización para el tratamiento dependiendo fundamentalmente de cuál sea la finalidad de dicha operación[683]. Y segundo, porque cuando la LOPD establece excepciones al consentimiento lo hace basándose en la finalidad del tratamiento: proteger un interés vital del interesado, el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias, realizar una investigación policial concreta, etc. En estos casos se reconocen situaciones en las que se tiene como fin la salvaguarda de bienes jurídicos de particular relevancia que merecen mayor protección que el derecho a dar el consentimiento. Precisamente, cuando el consentimiento no es requerido para llevar a cabo el tratamiento de los datos, y especialmente en los tratamientos realizados por las administraciones públicas, cuya actividad tiene que realizarse en todo caso en el ámbito de las competencias y potestades atribuidas a las mismas por el ordenamiento jurídico[684], el principio de la finalidad alcanza mayor importancia, pues se convierte en la principal garantía para el titular de los datos de que el tratamiento se va a realizar respetando sus derechos fundamentales[685]. En la medida en que una persona conoce que sus datos van a ser empleados para el cumplimiento de un fin concreto se asegura de que la información será manipulada en un ámbito determinado.

[679] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 81.
[680] GUICHOT, *Datos personales...*, cit., 2005, pp. 230-231; SANZ CALVO, "Calidad de los datos...", cit., 2008, p. 146.
[681], Artículo 5.1.a) LOPD; Artículo 10.b) Directiva 95/46/CE.
[682] Artículo 11.1 LOPD; Considerando 28 Directiva 95/46/CE.
[683] Artículo 6 LOPD; Artículo 7 Directiva 95/46/CE.
[684] SOUVIRÓN, "En torno a la Juridificación...", cit., 1994, p. 135; HERRÁN ORTIZ, *La Violación...*, cit., 1998, pp. 177-178.
[685] PÉREZ VELASCO, "Los Ficheros Públicos", cit., 2005.

Una vez aportada una definición del principio de finalidad, y señalada la especial importancia que se le otorga en las normas como criterio vertebrador de la regulación de este ámbito, hay que determinar las características que ha de cumplir dicha finalidad para que un tratamiento sea acorde a la Ley. Es aquí donde se aprecian las diferencias entre las distintas normas.

II.1.2. La necesidad de que la finalidad sea "determinada, explícita y legítima".

La LOPD exige que la finalidad que tiene que guiar el tratamiento de los datos sea "determinada, explícita y legítima" [686]. Para entender debidamente el sentido de estos conceptos es necesario atender a lo que otras normas han dispuesto sobre este mismo punto.

La actual regulación plantea cambios con respecto a la anterior. La derogada LORTAD simplemente exigía que la finalidad fuera "legítima"[687]. Con la norma actualmente vigente no basta con que la finalidad tenga esa cualidad de legítima, sino que tiene que ser, además, explícita, precisa y claramente identificada. En este sentido, se ha señalado en alguna memoria de la AEPD que la LOPD refuerza el principio de finalidad[688]. El tratamiento de los datos de los que una persona es titular sólo puede llevarse a cabo cuando se dirige a cumplir una finalidad determinada, explícita y legítima.

La redacción de la actual Ley es fruto de la trasposición de la Directiva europea, que recoge la necesidad de que la finalidad sea "determinada, explícita y legítima"[689]. Ya el Convenio del Consejo de Europa de 1981 reconocía más requisitos que los establecidos en la derogada Ley orgánica de protección de datos. Concretamente, exigía que esta finalidad fuera "determinada y legítima"[690]. La ratificación[691] y publicación de este Convenio en el BOE[692] debía haber llevado a la LORTAD a reconocer estas características[693]. No obstante, hasta la aprobación de la actual Ley orgánica de protección de datos no se han reconocido en el ámbito interno las garantías exigidas por las normas internacionales.

Cuando la Ley dispone que la finalidad tiene que ser "legítima", se entiende que se refiere a que ha de ser acorde a lo dispuesto en las normas. Una manipulación de datos que persiga una finalidad contraria a Derecho no será válida, independientemente de que esté amparada por el consentimiento del titular de los datos o se lleve a cabo de buena fe, para cumplir con un fin en principio beneficioso para dicho titular. Más allá de esta exigencia, en el caso de la Administración el cumplimiento del requisito de legitimidad se ve reforzado por el hecho de que

[686] Artículo 4.1, LOPD, que reproduce prácticamente lo que la Directiva 95/46 establece en su artículo 6.1.b). TRONCOSO REIGADA, "El Principio de Calidad…", cit., 2010, p. 342, realiza un interesante análisis de estos conceptos.
[687] Artículo 4.1 LORTAD.
[688] Memoria de la AEPD de 1999.
[689] Artículo 6.1.b) y Considerando 28 Directiva 95/46/CE.
[690] Artículo 5.b) Convenio 108/1981 del Consejo de Europa.
[691] Instrumento de ratificación de 27 de enero de 1984.
[692] BOE nº 274, 15 de noviembre de 1984.
[693] Artículo 96.1 CE; STC 20 de julio de 1993, FFJJ 5 y 6 y voto particular; SAIZ ARNAIZ, *La Apertura Constitucional...*, cit., 1999. Ni siquiera la fuerza interpretativa que se les reconoce a los tratados ratificados por el Estado en materia de Derechos Humanos en el artículo 10.2 CE hizo que la LORTAD recogiera dichas características a cumplir por el principio de finalidad.

toda actividad administrativa se ha de someter al principio de legalidad o juridicidad[694]. No es este el lugar donde se ha de analizar el contenido de estos conceptos. Baste con decir que en términos genéricos, de estos principios deriva la obligación de los órganos administrativos de no actuar más allá de lo que las normas dicten[695]. Los órganos administrativos sólo pueden ejercer las potestades atribuidas por las normas[696]. Aplicando estos criterios a lo que aquí interesa se deduce que cuando es la Administración, por ejemplo sanitaria, la que manipula datos de carácter personal, la finalidad a perseguir no sólo deberá ser legítima, sino que además deberá vincularse con las potestades que las normas atribuyen a dichos órganos[697].

La cualidad de "determinada" se refiere a que la finalidad ha de constituir un objetivo concreto. No puede referirse a un objetivo inexacto o inconcreto, sino que tiene que tratarse de un motivo cuyos contornos se puedan distinguir perfectamente. En algún caso la jurisprudencia ha asumido la equiparación de la cualidad de "determinada" con la de "muy específica"[698], lo cual da a entender que el grado de concreción ha de ser muy alto.

La exigencia de que sea "explícita" se refiere a que la finalidad pueda identificarse claramente. Más allá de que la finalidad que justifique la manipulación de datos tenga que ser determinada, es necesario que al titular de los datos se le presente la misma de forma inequívoca, sin ambigüedades ni fórmulas abstractas.

Estos requisitos tienen una importancia esencial, sobre todo a la hora de que el responsable del fichero haga efectiva la obligación de informar al titular sobre las características de la manipulación que va a llevar a cabo. Desde este punto de vista, se podría pensar que la inclusión de esos nuevos elementos, "determinada y explícita", en la Ley actual no ha sido completa. Nada dice la norma estatal sobre el grado de concreción que hay que exigir al responsable del fichero a la hora de determinar la finalidad. Lo cierto es que hubiese sido conveniente que la LOPD, desarrollando lo que establecen la Directiva europea y el Convenio, hubiera especificado este punto. El hecho de que la Ley no reconozca expresamente que la determinación y explicitud han de ser máximas podría llevar a entender que la finalidad puede definirse de una forma excesivamente genérica. Esto supondría dejar una puerta abierta para que el responsable del fichero asuma una definición amplia de la finalidad con la que va a emplear los datos de carácter

[694] REBOLLO PUIG, "Juridicidad, Legalidad…", cit., 1991, p. 65, distingue estos conceptos

[695] CHINCHILLA MARÍN, *La Desviación…,* cit., 1999, p. 69, en el mismo sentido afirma que en "toda actuación administrativa hay (...) un *por qué* y un *para qué*. La Administración actúa *porque* una norma la ha apoderado en ese sentido *para que* cumpla una finalidad de interés público concreta"; COSCULLUELA MONTANER, *Manual de Derecho…,* cit., 2001, p. 306: la "potestad entraña, así, un poder otorgado por el ordenamiento jurídico de alcance limitado o medido para una finalidad predeterminada por la propia norma que la atribuye, y susceptible de control por los Tribunales. La potestad no supone, en ningún caso, un poder de acción libre, según la voluntad de quien lo ejerce, sino un poder limitado y controlable"; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 396.

[696] GARCÍA ENTERRÍA y FERNÁNDEZ, *Curso de Derecho…,* cit., pp. 438-440, el "Derecho no es, para la Administración una linde externa que señale hacia fuera una zona de prohibición y dentro de la cual pueda ella producirse con su sola libertad y arbitrio. Por el contrario, el Derecho condiciona y determina, de manera positiva, la acción administrativa, la cual no es válida si no responde a una previsión normativa";

[697] TRONCOSO REIGADA, "El principio de calidad…", cit., 2010, p. 343.

[698] STSJ de Asturias 12 de septiembre 2005, FFJJ 3 y 14, en el que el Tribunal hace suyos los argumentos de la demandada Administración asturiana que lleva a cabo la equiparación entre los conceptos de "finalidad determinada" y "finalidad muy específica".

personal, lo que iría en detrimento de la seguridad jurídica del titular de los datos[699] y, por consiguiente, de su derecho a la autodeterminación informativa, pues su capacidad de control sobre dicha información se vería reducida.

Se puede interpretar, sin embargo, que la deficiente regulación de la LOPD en su artículo 4.1 a este respecto no es tal en la práctica, si se lleva a cabo una interpretación sistemática de toda la norma. Así lo ha comprendido también la jurisprudencia[700]. Si el derecho a la autodeterminación informativa se concreta en el derecho a controlar los datos de uno mismo, es fundamental que el titular de la información conozca la finalidad específica que justifica su uso. Cada tratamiento tiene que dirigirse necesariamente a una determinada finalidad, que tiene que concretar el responsable del fichero o del tratamiento, y sólo a esa finalidad. Si ésta no se presenta al titular con la máxima concreción no habrá control sobre la información. Si la finalidad es genérica se dejará al responsable del fichero un amplio margen de actuación. En la Ley parece reflejarse la voluntad del legislador de querer limitar la capacidad de actuación del responsable a la hora de manipular los datos. El hecho de incluir nuevos requisitos con respecto a la normativa anterior es indicativo de este hecho. Los datos deberán emplearse para conseguir una finalidad determinada y concretada al máximo, debiendo cancelarse los datos en el momento en que este objetivo se haya llevado a cabo o cumplido por parte del responsable del fichero[701].

II.1.3. La necesidad de que los datos no sean empleados para finalidades incompatibles a las que motivaron su recogida.

La LOPD, además de requerir que la finalidad a la que se va a destinar la manipulación de los datos sea legítima, determinada y explicita, exige también que no sean tratados con una finalidad incompatible a la que motivó su recogida[702]. Si la información fue recabada con un objetivo determinado sobre el que se informó al titular de los datos, luego no podrá ser manipulada con otro fin incompatible al inicial[703]. El uso del término "incompatible" en la norma ha generado un importante debate pues puede llevar a interpretar que suaviza, en comparación a lo que disponen otras normas, la exigencia de que la finalidad sea única y concreta.

---

[699] HERRÁN ORTIZ, "La Protección...", cit., 2001, apunta que "cuanto más general sea el fin determinado más difícil será controlar y vigilar si los usos posteriores de los datos son incompatibles con el fin inicialmente previsto". RUIZ CARRILLO, *La Protección*..., cit., 2001, p. 32, entiende que "el dueño del fichero a de informar de forma clara e inequívoca al afectado de:
-para qué se están recogiendo los datos; -qué uso se va a hacer de los datos; -en qué consiste el tratamiento; -cuando terminará el tratamiento; -la posibilidad o no de oponerse al objeto y fines que ha planteado el dueño del fichero o la persona que está recogiendo los datos".

[700] STSJ de Asturias 12 de septiembre 2005, FFJJ 3 y 14.

[701] Artículo 4.5 LOPD. Así se evita que diferentes datos recogidos en diferentes momentos y con diferentes finalidades se vayan almacenando (*datawarehouse*) y sean usados después, por ejemplo, para elaborar perfiles de los titulares de los datos (*datamining).*

[702] Artículo 4.2 LOPD.

[703] STC 13 de enero de 1998, FJ 4, en la que se advierte que unos datos sobre la afiliación sindical de unos trabajadores no pueden ser empleados con fin distinto al de descontar de la retribución la cuota sindical. Resolución APDCM, 23 de septiembre de 2009, "Utilización de los datos que constan en un fichero de usuarios del sistema sanitario de un centro de salud para fines incumplatibles con los que motivaron la recogida de datos", en la que se decide que unos datos contenidos en ficheros sanitarios, que fueron, evidentemente, recabados con el fin de salvaguardar la salud de una persona, no pueden ser empleados por un médico para interponer una denuncia contra dicho paciente.

Para determinar el alcance de este requisito es necesario ponerlo en relación con la anterior LORTAD y con la Directiva europea de 1995. Establecía la primera de estas normas que los datos no pueden emplearse para llevar a cabo "finalidades distintas" a las que motivaron su recogida[704]. Por su parte la Directiva señala que los datos no podrán ser tratados de "manera incompatible" con los fines que justificaron su recogida[705]. Estas expresiones son semejantes a la recogida por la actual LOPD. No obstante, las pequeñas diferencias que se encuentran entre las distintas redacciones de las normas hacen que tanto la derogada Ley como la norma europea deban ser tenidas en cuenta y analizadas para comprender correctamente el alcance de la expresión "finalidades incompatibles", empleada por la Ley estatal hoy vigente.

Como ya se ha puesto de manifiesto por la doctrina, la diferencia entre la vigente Ley y la anterior es evidente. La primera dispone que los datos no podrán usarse para finalidades "incompatibles" mientras que la segunda hablaba de finalidades "distintas"[706]. Se ha repetido constantemente, no sin justificación, que la norma actualmente vigente ha supuesto en este punto un paso atrás con respecto a la ya derogada[707], y es que resulta obvio que el concepto "incompatible" es menos riguroso o estricto que el de "distintas" y verdaderamente indeterminado[708]. Cuando se prohíbe el tratamiento de unos datos para finalidades incompatibles se permiten otros tratamientos para fines compatibles a pesar de que sean distintos[709]. Esta posibilidad conlleva, como se verá, consecuencias negativas desde el punto de vista del control por el titular de sus datos, fundamentalmente desde la perspectiva del respeto al principio de finalidad, que determina que cada tratamiento se deberá dirigir al cumplimiento de un objetivo determinado y explícito.

Parece que el cambio en la redacción se debe a la necesidad de la nueva norma de adaptarse a lo establecido en la Directiva europea que también emplea el término "incompatible". Sin embargo, hay que puntualizar que lo dispuesto en la LOPD y lo fijado por la norma comunitaria no se corresponden. La propia jurisprudencia ha puesto de manifiesto que "la transposición del término "incompatibles" resulta confusa y equívoca tal y como ha quedado plasmada en el derecho español"[710].

La norma comunitaria, siguiendo lo que ya fijaba el Convenio del Consejo de Europa[711], establece que los datos no podrán ser tratados "*de manera incompatible con dichos fines"* determinados, explícitos y legítimos para los que fueron recogidos. Aquí la compatibilidad se refiere al tratamiento, no a la finalidad. La finalidad no puede ser distinta. Lo que puede cambiar es la forma de manipular los datos. En la norma estatal, sin embargo, lo que puede cambiar es la

[704] Artículo 4.2 LORTAD
[705] Artículo 6.1.b) Directiva 95/46/CE.
[706] FREIXAS GUTIÉRREZ, *La Protección*..., cit., 2001, p. 153, entiende que con la sustitución del concepto distintas por el de incompatibles no "estamos ante una simple diferencia semántica sino que (...) estamos ante la quiebra del principio finalista que preveía la derogada LORTAD".
[707] REBOLLO DELGADO, *Derechos Fundamentales*..., cit., 2004, p. 147.
[708] DE MIGUEL SÁNCHEZ, *Tratamiento de Datos*..., cit., 2004, p. 55.
[709] TASCÓN LÓPEZ, *El Tratamiento por la Empresa…,* cit., 2005, p. 91, parece aprobar el cambio de concepto, en la medida en que la regulación actual otorga cierta flexibilidad a la hora de manipular información en el ámbito de la empresa, lo cual resulta, a criterio del autor, positivo.
[710] SSAN 17 de marzo de 2004, FJ 4, y 6 de abril de 2006, FJ 4.
[711] Artículo 5.b) Convenio 108/1981 del Consejo de Europa.

finalidad: puede manipularse la información para conseguir finalidades distintas, aunque con la condición de que sea compatible con el objetivo inicial. Se entiende aquí, con la doctrina y jurisprudencia, que la transposición de la Directiva no se ha hecho de manera adecuada debido a que se relajan las garantías dispuestas por la norma supranacional[712].

Es evidente que la LOPD supone una relajación de la norma con respecto a la LORTAD y a la Directiva. El empleo del concepto incompatible, en la forma en que lo hace la Ley actual, implica abrir la puerta a una posibilidad que atenta al núcleo esencial del derecho a la autodeterminación informativa[713]. Supone que los datos referentes a una persona determinada pueden ser empleados con fines distintos, aunque compatibles, a los que en un inicio inspiraron la recogida, ampliando así el ámbito en que los mismos datos pueden ser tratados[714]. Si los datos recogidos para llevar a cabo una finalidad pueden ser tratados por el mismo responsable, como parece sugerir la LOPD, para llevar a cabo una finalidad distinta pero compatible con la que motivó la recogida, es evidente que el control por parte del titular con respecto a sus datos de carácter personal disminuye. Los datos podrían ser empleados según esta interpretación, para una finalidad distinta a la que justificó su recogida y para la que, en concreto, el titular dio su consentimiento.

La jurisprudencia, consciente de la comentada situación, ha marcado una línea interpretativa en torno al término "finalidades incompatibles" que merece ser expuesta. Se podría decir que mediante argumentos empleados en diferentes sentencias consigue devolver a sus justos términos el sentido en el que hay que entender dicho concepto[715].

El punto de partida lo marca la idea de "que la interpretación del término <<incompatibles>> debe realizarse de forma sistemática poniéndose en relación dicha expresión con el principio de autodeterminación que inspira la Ley. Pues una interpretación amplia del término <<incompatibles>>, sin tener en cuenta dicho principio lo vaciaría de contenido"[716]. La interpretación del concepto "finalidades incompatibles" no puede llevarse a cabo, pues, de forma aislada respecto al resto de la norma. Partiendo de esta consideración la jurisprudencia ha tendido a equiparar los conceptos de "incompatible" y "distintas".

Primero, es consciente del riesgo que plantea la asunción de una interpretación literal del concepto "incompatible". Se parte del reconocimiento de la ambigüedad del término. Señala que "según el diccionario de la Real Academia <<incompatibilidad>> significa <<repugnancia que tiene una cosa para unirse con otra, o de dos o más personas entre si>>". Atendiendo a este significado concluye que "una interpretación literal ampararía el uso de los datos para cualquier fin abriendo una gama indefinida e ilimitada de finalidades, pues es muy difícil imaginar usos que

[712] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 94.
[713] SEOANE RODRÍGUEZ, "De la Intimidad...", cit., 2002, p. 161, concluye que la "compatibilidad de la finalidad aceptada por el art. 4.2 LOPD resulta contradictoria con la exigencia de determinación y explicitud –y legitimidad- de la finalidad para la que se han obtenido los datos de carácter personal presente en el artículo 4.1 LOPD. Determinada es lo mismo que definida, precisa, señalada con precisión; y explícita quiere decir que expresa clara y determinadamente una cosa. Por ello parece que la finalidad a la que se alude ha de ser una finalidad única"
[714] ULL PONT, *Derecho Público*..., cit., 2000, p. 119.
[715] VERDAGUER LÓPEZ y BERGAS JANÉ, *Prontuario protección*..., cit., 2009, p. 41.
[716] SAN 14 de junio de 2002, FJ 2.

produzcan la repugnancia que evoca la incompatibilidad, por lo que semejante interpretación conduce al absurdo y como tal ha de rechazarse". Una interpretación literal del concepto "incompatible" abriría la puerta a la posibilidad de que unos datos de carácter personal recogidos para una finalidad determinada se empleen para otras varias finalidades distintas pero compatibles.

Dando un paso más y basándose en el anterior argumento la jurisprudencia excluye la interpretación más extensiva a la que podría dar lugar el cambio de términos. Señala que el cambio de "distinto" por "incompatible" "no significa que el titular del fichero o del tratamiento pueda usar los datos a su antojo y conveniencia para finalidades distintas de las que motivaron la recogida de tales datos, a pesar de que dichas finalidades no sean contrarias e incompatibles con aquellas para las que los datos fueron recabados"[717]. Por lo tanto, se aboga, cuando menos, por una interpretación restrictiva del término "incompatibles".

Pero es más, atendiendo a la exigencia que la propia jurisprudencia se había marcado de interpretar el artículo 4.2 de la LOPD de manera conjunta con toda la norma, esta misma jurisprudencia da un último paso para concluir que aplicado "de forma literalista el artículo 4.2 de la Ley Orgánica quedaría privado de sentido y vaciado de contenido; y para evitar este resultado indeseable esta Sala considera que lo que prohíbe el precepto es que los datos de carácter personal se utilicen para una finalidad distinta de aquélla para la que han sido recogidos"[718]. Se acaba, por lo tanto, por equiparar los conceptos de "distintas" e "incompatibles". Se justifica esta conclusión poniendo acertadamente en relación el principio de finalidad y el de consentimiento. Cuando el titular de los datos da el consentimiento para que sus datos sean tratados, lo hace a sabiendas de que esa manipulación se llevará a cabo con una finalidad determinada, así, "cuando los datos se usen con otra finalidad distinta se precisará el consentimiento del afectado. Y no parece que el art. 4.2, venga a efectuar una ampliación sobre la posibilidad de utilización de los datos, como entiende el actor, porque ello supondría dejar sin contenido el art. 6.2, cuya redacción en este punto es igual a su homónimo de la Ley 5/92"[719].

La perspectiva que refleja esta jurisprudencia resulta también de una interpretación sistemática de la LOPD. Cuando la Ley entra a determinar las infracciones establece como infracción grave la recogida de datos con "finalidades distintas" de las que constituyen el objeto legítimo de la empresa[720]. El uso del término "distintas" en este apartado puede ser considerado como reflejo de que lo que se prohíbe en realidad no es otra cosa que el empleo de los datos de carácter personal con finalidades distintas a las que motivaron su recogida.

[717] SAN 6 de abril 2006, FJ 4.
[718] SAN 8 de marzo de 2002, FJ 6: "si la recogida se hizo con fines determinados, cualquier uso o tratamiento posterior con finalidad distinta es incompatible con la primera finalidad que determinó la captura por lo que, en este contexto, diferente o incompatible significan lo mismo"; STC de 30 de noviembre del 2000, FJ 13: "el derecho a consentir la recogida y tratamiento de los datos personales no implica en modo alguno consentir la cesión de tales datos a terceros... Y, por tanto, la cesión de los mismos a un tercero para proceder a un tratamiento con fines distintos de los que originaron su recogida, aun cuando puedan ser compatibles con éstos supone una nueva posesión y uso que requiere el consentimiento"; SAN 17 de marzo de 2004, FJ 4.
[719] SAN 8 de febrero 2006, FJ 3.
[720] Artículo 44.3.b) LOPD: Es infracción grave "*la recogida de datos de carácter personal (...) con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad*".

Por su parte, la autoridad competente para garantizar el cumplimiento de la LOPD ha llevado a cabo una interpretación del concepto "finalidades incompatibles" que parece ha ido evolucionando con el tiempo. En su memoria del año 2002 la AEPD entendía que dado "que la Ley no identifica qué ha de entenderse por <<fin compatible>>, debe analizarse la existencia de dicha compatibilidad en cada supuesto de hecho que se plantee, determinando si a la luz de las disposiciones aplicables a cada caso, y de las circunstancias del mismo, cabe considerar que esa finalidad que se alega como compatible resulta lícita a la luz de las normas aplicables y si la misma guarda una adecuada relación con la finalidad que justificó el tratamiento de los datos"[721]. Parece deducirse que la memoria asume aquí el criterio de la incompatibilidad aceptando que los mismos datos puedan ser manipulados con fines distintos aunque compatibles, si bien lo hace planteando garantías añadidas. Según esta interpretación, la finalidad puede ser distinta pero compatible, siempre y cuando guarde una relación adecuada con la finalidad inicial que motivó la recogida de los datos. Se perciben, por lo tanto, las dudas que la agencia estatal de protección de datos tenía al respecto del uso en la LOPD del concepto "incompatibles".

En la actualidad, siguiendo la línea interpretativa de la jurisprudencia que se ha citado, esta institución ha concluido en alguna de sus resoluciones que "si el tratamiento ha de ser "pertinente" al fin perseguido y la finalidad ha de estar "determinada", difícilmente se puede encontrar un uso del dato para una finalidad "distinta" sin incurrir en la prohibición del artículo 4.2 aunque emplee el término "incompatible""[722].

La justificación de la incorporación del concepto incompatible en el articulado de la LOPD salió a la luz en el debate parlamentario que precedió a la aprobación de dicha norma. Más allá de argumentos puramente jurídicos que podían fundamentarse en la necesidad de trasponer la Directiva europea, se emplearon razones de carácter sustantivo que merecen ser comentadas.

El Grupo Parlamentario Vasco señaló, que "utilizamos la palabra "incompatible" porque es la misma palabra que utiliza la Directiva comunitaria en su artículo 6.1 apartado b). En un ejemplo muy claro, un banco tiene datos de sus clientes con la finalidad de ofrecerles servicios financieros. Si este banco decidiese además ofrecerles a sus clientes un cierto tipo de seguro, este seguro tendría una finalidad distinta de aquélla para la que los datos fueron recogidos, que fue para ofrecer servicios financieros. En cambio en la Directiva sí se permitiría este caso, puesto que el banco ofrece un seguro a sus clientes, no se considera finalidad incompatible con la inicial.

Las empresas, a lo largo de su historia, van añadiendo actividades a su objeto inicial. Por ejemplo, a la venta de libros pueden añadir la venta de cursos a distancia, pero esto no es incompatible con la finalidad primera, en cambio sí es una finalidad distinta. Con la actual redacción, estaría prohibido utilizar la base de datos propia de clientes con una finalidad distinta, aunque fuera una finalidad compatible con la actividad inicial de la compañía. Creemos que

[721] Memoria de 2002 de la AEPD, p. 292.
[722] Resolución de la AEPD, R/00485/2004 del 8 de septiembre de 2004, procedimiento AAPP/00011/2004.

debemos tomar el texto de la Directiva y no restringir más de lo necesario la actividad de las empresas españolas"[723].

Frente a esta postura, que en última instancia fue la que prevaleció, en ese mismo debate parlamentario se defendió también la posición contraria, que abogaba por cambiar el concepto "incompatibles", que aparecía en el proyecto de Ley, por el de "distintas" que ya recogía la LORTAD[724]. La necesidad de transponer la Directiva europea, como se ha dicho, erróneamente entendida, acabó por justificar una regulación que, interpretada de manera literal, podría vulnerar el sentido mismo del derecho a la autodeterminación informativa.

Ante las numerosas críticas que se han suscitado en torno a esta regulación se ha planteado en alguna ocasión reformar la Ley hoy vigente. Tanto desde movimientos sociales[725], como en sede parlamentaria[726] se ha propuesto sustituir el concepto "incompatibles" por el de "distintas", retornando a la forma establecida por la LORTAD. Sin duda puede entenderse que esta es una opción acertada, pues devolvería la regulación a sus justos términos[727].

Después de atender a las diferentes interpretaciones que se han llevado a cabo en torno al empleo por la LOPD de la expresión "finalidades incompatibles", y analizar los problemas que la misma plantea, la conclusión que se extrae no puede ser otra que la que sigue. La inclusión del concepto "incompatibles" no tiene justificación alguna. En primer lugar porque se trata de un concepto impreciso que podría llegar a dar cobertura, dependiendo de la interpretación que se haga del mismo, no sólo a prácticas aceptables como las descritas por el Grupo Parlamentario Vasco en el debate sobre la aprobación de la Ley, sino también a actuaciones más agresivas que en modo alguno podrían estar justificadas. Y en segundo lugar, porque la posibilidad de que el responsable del tratamiento tenga la capacidad de emplear los datos de carácter personal con una finalidad distinta a la que en un inicio motivó la recogida de dichos datos, trasladaría el ámbito de decisión y control sobre los datos del titular de los mismos al indicado responsable, lo que podría suponer una clara violación del derecho fundamental a la autodeterminación informativa. El titular da su consentimiento para que estos sean tratados con una única finalidad, y el responsable del fichero no puede interpretar esa voluntad para entender que acepta un uso diferente de dichos datos con una finalidad distinta, por compatible que sea. Sólo el titular de los

[723] BOCG nº 135-7, Serie A, de 4 de noviembre de 1998. Enmienda número 19.
[724] BOCG nº 135-7, Serie A, de 4 de noviembre de 1998: Enmienda nº 102 defendida por el Grupo Mixto.
[725] Navegante.com, jueves 3 de marzo de 2005, en http://www.elmundo.es/navegante/. En este artículo se hace mención a la postura de La CLI (Comisión de Libertades e Informática) a favor del cambio de la redacción de la LOPD.
[726] BOCG. Congreso de los Diputados, nº 278-1, 18 de octubre de 2002, se recoge la postura del PSOE al respecto, favorable al cambio de la LOPD:
[727] Merece la pena reproducir los argumentos dados por la CLI para justificar la modificación de la redacción de la LOPD en el 4.2 con la intención de recuperar el concepto "distintas": "La esencia de todo el sistema de protección de los datos de carácter personal, es que el titular de los mismos tenga la seguridad de que la recogida de sus datos tiene una finalidad legítima concreta, de la que debe ser informado previamente al amparo del artículo 5.1 de la misma Ley, y que sus datos serán utilizados con esta concreta finalidad y no otra. En otro caso perdería además toda virtualidad y eficacia la posibilidad de ejercitar los derechos de acceso, rectificación o cancelación de los datos, al no poder tener la certeza de para qué se utilizan éstos".
"Si los responsables de tratamiento disponen que los datos recogidos para un determinado fin sean aplicados a otro distinto –por muy compatible que sea- se está anulando el original consentimiento del interesado y obviando el necesario para ese nuevo fin".

datos, o una causa reconocida por ley, puede fundamentar el uso de los datos con otra finalidad a la que motivó la recogida. Tanto es así que normas de reciente aprobación dirigidas a la regulación de sectores que afectan a la protección de datos de carácter personal han retomado el concepto de "finalidades distintas"[728].

En este sentido, resulta cuando menos sorprendente que el reglamento que desarrolla la LOPD no haya introducido los criterios dados por la jurisprudencia y la AEPD para interpretar este concepto, manteniendo el término "incompatible".

II.2. La protección de la salud como bien jurídico que choca con el derecho a la autodeterminación informativa.

Se han analizado hasta ahora los requisitos que exige la normativa reguladora de la protección de datos de carácter personal para que una finalidad sea acorde a la Ley. Deberá ser legítima, determinada y explícita. Además, una vez recabados los datos no podrán ser manipulados para llevar a cabo una finalidad distinta a la que motivó esa recogida.

En el estudio que aquí se realiza se analiza el tratamiento de los datos de carácter personal en un ámbito muy concreto, como es el sanitario, con una finalidad determinada, la de proteger la salud de las personas. Se ponen en relación dos derechos con diferente naturaleza jurídica: el derecho fundamental a la autodeterminación informativa y el derecho a la protección de la salud, que se reconoce en la CE como principio rector de la política social y económica. Estos dos derechos pueden entrar en conflicto en este ámbito. El tratamiento de datos sanitarios es necesario para proteger la salud de las personas. Hay que preguntarse hasta qué punto puede esa finalidad justificar la limitación del derecho a la autodeterminación informativa, por ejemplo, posibilitando que la información referente a una persona sea manipulada sin su consentimiento. Para resolver este interrogante es necesario, antes de nada, profundizar en dos cuestiones. En primer lugar se intentará determinar si puede considerarse el derecho a la protección de la salud un bien jurídico de suficiente entidad como para limitar el derecho fundamental a la autodeterminación informativa. Después, se tratará de concretar qué elementos completan la genérica finalidad de la protección de la salud, es decir, en qué consiste la protección de la salud.

II.2.1. Caracterización jurídica de los principios rectores de la política económica y social en la Constitución.

II.2.1.A. Los principios rectores de la política social y económica como expresión del Estado social. Referencia a las diferencias tradicionalmente reconocidas entre principios rectores y derechos fundamentales.

En el ámbito sanitario la manipulación de datos no constituye una finalidad en sí misma, sino que se trata de un instrumento utilizado para alcanzar una finalidad determinada: la protección de la salud de las personas. Cabe preguntarse si el cumplimiento de este fin puede llegar a limitar

[728] Artículo 5.3 Ley 14/2007, 3 de julio de 2007, de Investigación Biomédica.

alguna de las facultades que completan el derecho fundamental a la autodeterminación informativa.

El derecho a la protección de la salud se recoge en la Constitución como un principio rector de la política económica y social. Por el contrario, el derecho a la autodeterminación informativa ha sido reconocido expresamente por el TC como un derecho fundamental autónomo[729]. Las mayores garantías que se otorgan en la norma suprema a los derechos fundamentales llevan a preguntarse si el derecho a la protección de la salud constituye un bien jurídico suficiente para limitar dicho derecho. Como se verá, existen argumentos para contestar en sentido afirmativo.

En un contexto histórico-social determinado comienzan a incorporarse y reconocerse en los textos jurídicos los que hoy día son calificados, con mayor o menor fortuna[730], como derechos sociales, entre los que se encuentra el derecho a la protección de la salud. El contenido y las características de estos derechos vienen marcados precisamente por ese contexto. Tomando como fundamento sus particularidades la Constitución española los ha recogido, en su gran mayoría, en un apartado concreto con el calificativo de "principios rectores de la política económica y social", otorgándoles, *a priori*, un régimen distinto al dado a los demás derechos. Más allá de las críticas que se puedan hacer a esta distinción y a la consideración de estos principios rectores como derechos de segundo rango o categoría[731], se entiende necesario exponer brevemente el citado contexto para comprender mejor el alcance del derecho a la protección de la salud.

Con la lucha por la mejora de las condiciones sociales y económicas llevada a cabo sobre todo por la clase obrera y su incorporación a la actividad parlamentaria, comienza, tras la Primera Guerra Mundial, un proceso de positivación de los denominados derechos económico-sociales[732]. Los derechos a una vivienda digna, al medio ambiente, a la salud, al trabajo en unas condiciones mínimas de calidad, a la educación, etc., que se dirigen a mejorar la calidad de vida en sociedad de todos los ciudadanos, empiezan a reconocerse por los legisladores de los diferentes estados. Se trata de garantizar lo que se ha llamado, completando la clasificación que Jellinek hiciera en su día, el "status social y económico de los ciudadanos"[733].

Se ha entendido que estos derechos presentan como particularidad principal que exigen para su efectiva realización la actividad de los poderes públicos. Desde un punto de vista, quizás, tradicional[734] han sido calificados, en este sentido, como derechos prestacionales[735]. Así, el Estado, en la medida en que lleva a cabo estas actuaciones dirigidas a hacer efectivos esos

[729] STC 30 de noviembre del 2000, FFJJ 4, 5 y 6.
[730] PÉREZ LUÑO, *La Tercera…,* cit., 2006, p. 293.
[731] ABRAMOVICH y COURTS, *Los Derechos Sociales…,* cit., 2002.
[732] GÓMEZ-REINO CARNOTA, "Las Libertades...", cit., 1978, p. 37; GARCÍA MACHO, "Los Derechos Fundamentales Sociales…", cit., 2009, pp. 72-73.
[733] LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit.,2002, p. 147.
[734] GARCÍA MACHO, "Los Derechos Fundamentales Sociales…", cit., 2009, pp. 69-70.
[735] GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp 129-130; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 438-439.

derechos sociales[736], adquiere el calificativo de Estado social[737], concepto que comienza a emplearse a partir de 1929[738].

El Estado español se reconoce en la propia Constitución como Estado Social y Democrático de Derecho[739]. El empleo de esta fórmula en la caracterización política del Estado ha sido cuestionado, pues no queda claro según parte de la doctrina el contenido que hay que dar a cada una de las calificaciones de "democrático", "social" y "de Derecho". Se ha dicho, por ejemplo, que la consideración del Estado como "democrático" necesariamente incluye la consideración de ese mismo Estado como "social" [740]. En todo caso la calificación del Estado español como "social" queda expresamente recogida.

Son varias las características que definen este modelo de Estado[741]. Sin embargo, en este momento basta con señalar que este reconocimiento supone principalmente, como han afirmado prácticamente todos los autores, la adquisición del compromiso por parte de los poderes públicos de poner todos los medios posibles para hacer efectiva la que se ha venido en llamar "igualdad material o real"[742], y, en última instancia, garantizar las condiciones adecuadas para que la dignidad de las personas se vea protegida y promocionada[743]. Frente a la igualdad formal proclamada por la norma suprema, que se refiere a la igualdad de trato ante la Ley, de tal forma que en situaciones iguales todos tienen que ser tratados de la misma forma tanto en la legislación como en su propia aplicación[744], la igualdad material va más allá y reclama, en uno de sus aspectos, una actuación positiva de los poderes públicos dirigida a establecer unas condiciones mínimas de equilibrio de situaciones sobre todo socio-económicas para todos[745]. El Estado se obliga a hacer todo lo posible para que desaparezcan las desigualdades que en una sociedad nacen como consecuencia de diferentes motivos, principalmente económicos[746]. Los poderes públicos, sea cual sea la configuración del parlamento en un momento determinado, están obligados a poner todos los medios posibles para hacer efectivos los derechos sociales que se reconocen en la CE y, con ello, a la mejora de la calidad de vida de los ciudadanos en aspectos como los citados[747]. Una visión más moderna de estos derechos los ha vinculado no sólo al principio de igualdad material sino también al principio de libertad. Su reconocimiento en

[736] CARMONA CUENCA, *El Estado...,* cit., 2000, p. 150, hace referencia a la definición que Maziiotti da de los derechos sociales: "los *derechos sociales* se entienden como los derechos de cualquier ciudadano a una directa o indirecta prestación positiva por parte de los poderes públicos, en función de la participación en los beneficios de la vida en sociedad, o de la actuación del principio de igualdad".
[737] PÉREZ LUÑO, *Los Derechos...,* cit., 1984, p. 184; SÁNCHEZ GOYANES, *Constitución Española...,* cit., 2005, p. 51.
[738] GARRORENA MORALES, *El Estado...*, cit., 1984, pp. 33-34.
[739] Artículo 1.1 CE.
[740] PÉREZ ROYO, *Curso de Derecho...,* cit., 1997, pp. 193-195.
[741] CARMONA CUENCA, *El Estado...*, cit., 2000, p. 119-120..
[742] BASSOLS COMA, "Los Principios...", cit., 1978, pp. 142-143; GARRORENA MORALES, *El Estado...*, cit., 1984, p. 48-56 y pp. 65-66; GARRIDO GUTIÉRREZ, "El Valor...", cit., 1994, p. 223-225; SUÑÉ LLINAS y VILLAR PALASÍ, "El Estado...", cit., 1996, pp. 512-513; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, p. 38-39; CIDONCHA, *La libertad…,* cit., 2006, p. 89.
[743] GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 106-107.
[744] Artículo 14 CE. STC 14 de julio de 1982, FJ. 2. PÉREZ LUÑO, *Dimensiones de la Igualdad...*, cit., 2005, pp. 19-22.
[745] Artículo 9.2 CE. PÉREZ LUÑO, *Dimensiones de la Igualdad...*, cit., 2005, pp. 44-45.
[746] GÓMEZ-REINO CARNOTA, "Las libertades...", cit., 1978, p. 38.
[747] GARRORENA MORALES, *El Estado...,* cit., 1984, pp. 82-84.

el texto constitucional no sólo se dirigiría a garantizar dicha igualdad, sino a fomentar una situación en que todo ciudadano pudiera llevar a cabo su vida en libertad, para lo cuál es necesario que los denominados derechos sociales sean efectivos[748].

En el ordenamiento interno el carácter social del Estado ha venido de la mano del reconocimiento expreso en la Constitución de una serie de derechos de contenido social. Si bien es verdad que a lo largo de su articulado son recogidos empleando diferentes fórmulas, incluso en algún caso como el del derecho a la educación otorgándoles la categoría de derecho fundamental, estos derechos sociales se regulan principalmente en el Capítulo III del Título I de la CE bajo la denominación de "Principios rectores de la política social y económica"[749].

La naturaleza jurídica de estos principios y su estatus dentro del sistema constitucional ha sido una cuestión muy debatida por la doctrina y se han mantenido posturas muy diferentes. Hay autores que han considerado que los principios rectores constituyen derechos fundamentales[750]. Han entendido, que a pesar de que las garantías otorgadas a estos principios son más laxas que las que salvaguardan la eficacia de los derechos fundamentales, interpretados *stricto sensu*, la integración de los principios rectores en el Título I, referente a los derechos y deberes fundamentales, los convierte también en fundamentales. Parece que en algún caso también se ha pretendido otorgarles ese carácter de fundamental por su relación con derechos que expresamente son catalogados en la Constitución como fundamentales. Es el caso, por ejemplo, del derecho a la protección de la salud, vinculado con la dignidad de las personas, el derecho a la vida o el derecho a la integridad física y moral[751]. No obstante, para la mayoría los principios rectores no son a efectos jurídicos y desde el punto de vista constitucional derechos fundamentales[752]. El carácter de estos principios como derechos subjetivos se ha puesto en duda[753]. Se ha argumentado que no pueden ser considerados derechos debido a los problemas que genera la ejecución efectiva de los mismos en la realidad.

Más allá de este debate, lo que interesa es determinar cuál es el régimen jurídico de estos principios. Tradicionalmente, desde una perspectiva liberal, se ha tratado de marcar una distinción entre los principios rectores de la política social y económica y los demás derechos, tanto desde el punto de vista de sus garantías jurídicas y jurisdiccionales como desde el punto de vista de su eficacia[754]. La base de dicha distinción se ha fundamentado principalmente en los siguientes argumentos.

[748] GARCÍA MACHO, "Los Derechos Fundamentales Sociales…", cit., 2009.
[749] PRADA FERNÁNDEZ DE SANMAMED, "Revisión de los principios…", cit., 2003, p. 277; SÁNCHEZ GOYANES, *Constitución Española...*, cit., 2005, p. 50.
[750] GONZÁLEZ MORENO, *El Estado Social...*, cit., 2002, pp. 127-129.
[751] BRAGE CAMAZANO, *Los límites...,* cit., 2004, pp. 248-249; PÉREZ-LUÑO, *La Tercera Generación…,* cit., 2006, pp. 311-319.
[752] GARRIDO GUTIÉRREZ, "El valor constitucional…", cit., 1994, p. 215; CIDONCHA, *La libertad de Empresa…,* cit., 2006, pp. 93-94.
[753] RODRÍGUEZ DE SANTIAGO, "Artículo 53.3…", cit., 2008, p. 1.188. STC, 14 de febrero de 1991, FJ 5.
[754] PÉREZ LUÑO, *Los Derechos...*, cit., 1984, pp. 203-206 y pp. 213-214; PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 187-189; PRADA FERNÁNDEZ DE SANMAMED, "Revisión de los principios…", cit., 2003, pp. 279-280;

Por un lado, el contenido y la forma que adquieren los diferentes principios rectores es realmente diversa o variada: mandatos dirigidos a los poderes públicos, derechos, principios, etc[755]. Por otro lado, para alcanzar su plena eficacia jurídica estos preceptos necesitan de la actividad del legislador dirigida a concretar el contenido de los principios que se recogen en ellos[756]. En este sentido, se ha planteado la dificultad de determinar un contenido estable de estos principios. Por último, teniendo en cuenta que tratan de materias conflictivas, con una carga ideológica especialmente alta[757], referidas a cuestiones sobre las que recaen formas muy diferentes de entender la política y la realidad en general, constituyen disposiciones que necesariamente tienen que adquirir una forma especialmente vaga o indeterminada en la que quepan, atendiendo al principio democrático, ideologías y proyectos políticos diferentes, incluso contrapuestos. Además, su realización depende de factores tales como la capacidad económica que el Estado pueda tener en cada momento determinado, con lo que predefinir un catálogo concreto de prestaciones como contenido estable de los principios rectores parece imposible[758].

Los fundamentos de esta distinción, sin embargo, no son tan sólidos como se ha pretendido exponer en algún caso. La práctica demuestra que los problemas que plantean los derechos fundamentales y los principios rectores no son tan distintos en muchos casos. En ambos bloques se recogen realidades muy variadas que presentan problemas semejantes[759]. Es por ello que se ha llegado a afirmar, no sin razón, que el único motivo que ha llevado a dar un tratamiento diferenciado a los derechos fundamentales y a los principios ha sido únicamente la voluntad del constituyente. No existe, por lo demás, criterio objetivo alguno que obligue a un tratamiento distinto entre dos derechos de carácter eminentemente prestacional como el derecho a la educación y el derecho a la protección de la salud, el primero considerado como derecho fundamental y el segundo como principio rector[760]. Más allá de las discutibles diferencias de carácter histórico y ontológico que se acaban de citar entre ambas categorías[761], las más relevantes distinciones se han tratado de establecer partiendo de la Constitución, que ha otorgado a los principios rectores una regulación particular.

De inicio parece clara la voluntad del constituyente de otorgar un tratamiento diferente a los derechos fundamentales y a los principios rectores[762]. Es indicativo de ello el hecho de que estos principios ni siquiera sean calificados como derechos en el enunciado del Capítulo III de la CE[763]. La distinción entre ambas figuras se refleja sobre todo en las diferentes garantías que otorga la

[755] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 191; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 439 y 444; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 69-70 y pp. 160-162

[756] Articulo 53.3 CE: "*El reconocimiento, el respeto y la protección de los principios reconocidos en el Capítulo III informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos. Sólo podrán ser alegados ante la Jurisdicción ordinaria de acuerdo con lo que dispongan las leyes que los desarrollen*".

[757] LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 445.

[758] BALAGUER CALLEJÓN, *Derecho Constitucional...*, cit., 2003, p. 246.

[759] CARMONA CUENCA, *El Estado...*, cit., 2000, pp. 151-152.

[760] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 190.

[761] PISARELLO, *Los Derechos Sociales...*, cit., 2007.

[762] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 185; PÉREZ ROYO, *Curso de Derecho...*, cit., 1997, p. 281; SÁNCHEZ GOYANES, *Constitución Española...*, cit., 2005, p. 105.

[763] GARRIDO FALLA, "Comentario al...", cit, 2001, p. 986.

norma suprema a los dos grupos[764]. Sobre los principios no recae la reserva de Ley orgánica que existe para los derechos fundamentales. De la Constitución podría desprenderse que los principios no cuentan con un contenido esencial a respetar por la ley[765]. Se deduce que no se reconoce para estos principios la tutela por un procedimiento basado en los principios de sumariedad y preferencia. Tampoco se reconoce para ellos la posibilidad de que sean protegidos en amparo ante el Tribunal Constitucional.

La principal diferencia, sin embargo, desde la citada perspectiva tradicional, es que los principios sólo podrán alegarse ante la jurisdicción ordinaria si previamente han sido desarrollados y concretados por el legislador[766]: sin previo desarrollo a través de la actuación del legislador[767], del contenido que la CE reconoce a dichos principios no pueden deducirse derechos subjetivos[768]. La eficacia de estos preceptos a la hora de exigir o reivindicar derechos específicos depende de la actuación del legislador[769]. Las facultades concretas surgirán cuando el legislador desarrolle los enunciados recogidos en la Constitución. El legislador es el principal destinatario de estos mandatos[770]. Se trata de derechos de configuración legal[771]. El mandato al legislador para que desarrolle los preceptos contenidos en los principios rectores constituye por lo tanto una reserva de Ley[772]. El legislador debe regular estas materias para que los ciudadanos puedan reconocer en ellas facultades concretas[773].

Se estaría asumiendo con esta interpretación de los principios rectores, que de los enunciados que recoge la CE al referirse a los mismos no derivan directamente derechos o facultades subjetivas concretas que puedan alegarse ante los Tribunales y Jueces y demás poderes públicos[774]. El derecho a la vivienda, no reconocería, así, el derecho *stricto sensu* a obtener una vivienda digna, sino la obligación o el mandato a los poderes públicos, entre ellos al

[764] STSJ de Navarra 7 de marzo del 2000, FJ 3.
[765] Artículo 53 CE: *1. Los derechos y libertades reconocidos en el Capítulo II del presente Título vinculan a todos los poderes públicos. Sólo por ley, que en todo caso deberá respetar su contenido esencial, podrá regularse el ejercicio de tales derechos y libertades, que se tutelarán de acuerdo con lo previsto en el artículo 161.1.a)*
2. Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección 1ª del Capítulo II ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional. Este último recurso será aplicable a la objeción de conciencia reconocida en el artículo 30".
[766] Artículo 53.3 CE.
[767] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 195; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, pp. 148-149 y p. 446; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, p. 55, y p. 57.
[768] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 192.
[769] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 198.
[770] PÉREZ ROYO, *Curso de Derechos...*, cit., 1997, p. 196; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 445.
[771] LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 444.
[772] PÉREZ ROYO, *Curso de Derechos...*, cit., 1997, p. 359.
[773] BALAGUER CALLEJÓN, *Derecho Constitucional...*, cit., 2003, p. 25.
[774] GARRIDO GUTIÉRREZ, "El Valor...", cit., 1994, p. 228; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit, 2002, pp.142-143.

legislador, para que pongan todos los medios para que ese derecho se pueda hacer efectivo en la mayor medida posible[775].

Entendiéndolos así, como ha señalado gran parte de la doctrina, los principios no serían otra cosa que mandatos dirigidos a los poderes públicos, especialmente al poder legislativo, que tiene que desarrollar los enunciados genéricos establecidos por la Constitución[776].

II.2.1.B. Sobre la fuerza vinculante de los principios rectores de la política social y económica.

En algún caso se ha llegado a decir que los principios rectores de la política social y económica identifican un "horizonte utópico" hacia el que los poderes públicos han de dirigir sus actividades y esfuerzos[777]. Nada más lejos de la realidad. Se entiende aquí que estos principios no constituyen meros ideales hacia los que discrecionalmente pueden dirigirse los poderes públicos, sino que tienen una fuerza vinculante mayor de la que pueda intuirse de las consideraciones realizadas hasta ahora[778].

Se ha interpretado que los principios rectores constituyen meros principios programáticos y que no son directamente invocables ante los Jueces y Tribunales[779]. No obstante, parece asumido hoy día que estos principios, por sí mismos, no carecen de valor y eficacia jurídica alguna[780]. Una cosa es que, como se ha dicho, del contenido de sus enunciados no resulten directamente facultades concretas y otra que se entienda que constituyen simples normas programáticas, entendiendo por carácter programático, tal y como parece haberlo hecho en alguna ocasión el TC[781], normas que no vinculan a los poderes públicos y que no se pueden invocar ante los Jueces y los Tribunales. Hay que afirmar con rotundidad que estas disposiciones no son meros principios programáticos carentes de fuerza vinculante[782].

En la medida en que estos principios forman parte del contenido de la Constitución, todo sujeto, sea público o privado, está vinculado a los mismos[783]. El debate en torno al carácter normativo o retórico de toda la CE ha sido ya superado, y se admite inequívocamente que todo el contenido de esta norma tiene valor normativo[784], si bien es cierto que no todos los preceptos

[775] PÉREZ ROYO, *Curso de Derecho...*, cit., 1997, p. 281; PISARELLO, ", El Derecho a la Vivienda…", cit., 2009, p. 6.
[776] COBREROS MENDAZONA, *Los Tratamientos*..., cit., 1988, pp. 169-170; JIMÉNEZ CAMPO, "Comentario al artículo...", cit., 1996, pp. 520-522.
[777] SÁNCHEZ GOYANES, *Constitución Española*..., cit., 2005, p. 51.
[778] PISARELLO, ", El Derecho a la Vivienda…", cit., 2009; CUBERO MARCOS, "Derechos sociales…", cit., 2010, p. 352.
[779] GARRIDO FALLA, "Comentario al artículo...", cit., 2001, pp. 31-32 y pp. 975-977.
[780] LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 444-445; LARRAZABAL BASAÑEZ, *Curso de Derecho…,* cit., 2008, pp. 508-509.
[781] JIMÉNEZ CAMPO, "Comentario al artículo...", cit., 1996, p. 525, en la que hace referencia a la STC, 21 de junio de 1990, FJ. 4.
[782] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 193-194.
[783] Artículo 9.1 CE. SÁNCHEZ MORÓN, "Función Administrativa...", cit., 1984, p. 648; GARRIDO GUTIÉRREZ, "El Valor Constitucional...", cit., 1994, p. 215; JIMÉNEZ CAMPO, "Comentario al artículo...", cit., 1996, pp. 522-524.
[784] GARCÍA de ENTERRÍA, *La Constitución...*, cit., 2006, pp. 74-77; LASAGABASTER HERRARTE, *Fuentes del Derecho…,* cit., 2007, p. 37.

que la componen tienen las mismas características[785]. Así, los principios rectores, como parte de este contenido, no son meros programas sin valor jurídico, sino que tienen eficacia jurídica[786], aunque ésta sea atenuada con respecto a otras disposiciones como las que recogen los derechos fundamentales. Desde muy temprano el TC admitió que todos los principios y derechos constitucionales vinculan a todos los poderes públicos y son origen de derechos y obligaciones y no principios programáticos[787].

En primer lugar, como disposiciones que vinculan a todos los poderes públicos, no cabe duda que los principios rectores constituyen parámetros de interpretación que en todo momento se han de tener en cuenta a la hora de aprobar, aplicar o enjuiciar cualquier norma[788]. Así lo reconoce la propia Constitución cuando dispone que estos principios "*informarán la legislación positiva, la práctica judicial y la actuación de los poderes públicos*"[789], y así lo ha afirmado también la jurisprudencia[790]. La cláusula del Estado social y estos principios, que son el desarrollo de dicha cláusula, responden a una forma de entender la realidad, a unos valores concretos que en todo caso han de informar la creación y aplicación del Derecho, sobre todo, como ha señalado algún autor, a la hora de ponderar diferentes bienes jurídicos reconocidos por la propia Constitución[791]. Esta consideración tiene especial importancia para el legislador, que es quien tiene el deber de aprobar las normas más relevantes que afectan a los ciudadanos. El legislador no podrá desatender los mandatos que le imponen estos principios, y tendrá que tener en cuenta su contenido a la hora de aprobar las normas. Estos principios, por lo tanto, limitan la discrecionalidad del legislador, que no podrá ir contra los mismos[792].

Y en segundo lugar, más allá de esta función hermenéutica que se les atribuye, y a pesar del hecho de que según la Constitución de estos principios no derivan directamente derechos subjetivos, se reconoce la posibilidad de invocarlos de forma directa ante los poderes públicos[793]. Primero, como se ha venido realizando por la propia jurisprudencia[794] y ha admitido la doctrina[795], el empleo de estos principios se puede llevar a cabo poniéndolos en relación con derechos u otros principios fundamentales recogidos en la Constitución, como el principio de igualdad, la dignidad, etc. Segundo, si bien la aplicabilidad directa de estos principios puede entenderse

[785] GARRIDO GUTIÉRREZ, "El valor constitucional…", cit., 1994, p. 215.
[786] PRADA FERNÁNDEZ DE SANMAMED, "Revisión de los principios…", cit., 2003, p. 292.
[787] STC 23 de abril de 1982, FJ 8.
[788] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, p. 195; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 62-63.
[789] Artículo 53.3 CE.
[790] STC 5 de mayo de 1982, FJ 6; STSJ de Andalucía 11 de diciembre de 2000, FJ 7.
[791] DIEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 67.
[792] LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 445.
[793] SUÑÉ LLINAS y VILLAR PALASÍ, "El Estado...", cit., 1996, p. 491.
[794] SSTC, 20 de febrero de 1989, FJ 4: "No cabe excluir que la relación entre alguno de esos principios y los derechos fundamentales (...) haga posible un examen de este género cfr., por ejemplo, nuestra STC 155/1987 (...), ni, sobre todo, que el principio rector sea utilizado como criterio para resolver sobre la constitucionalidad de una acción positiva del legislador, cuando ésta se plasma en una norma de notable incidencia sobre la entidad constitucionalmente protegida" y 22 de mayo de 2006, FJ 8.
[795] GARRIDO GUTIÉRREZ, "El valor constitucional…", cit., 1994, p. 221; JIMÉNEZ CAMPO, "Comentario al artículo...", cit., 1996, p. 524; LÓPEZ GUERRA, ESPÍN, GARCÍA MORILLO, PÉREZ TREMPS, SATRUSTEGUI, *Derecho Constitucional...*, cit., 2002, p. 447.

limitada, esto no quiere decir que dichos preceptos no puedan constituir parámetros de constitucionalidad para el enjuiciamiento de otras normas. La indeterminación de los preceptos que componen el Capítulo III, la forma gramatical que los caracteriza, de mandato la mayoría de las veces, y la redacción del artículo 53.3 CE, hacen, en principio, difícil que éstos sean empleados como único argumento para decretar la inconstitucionalidad de una norma[796]. En este sentido, la jurisprudencia ha afirmado en alguna ocasión que parece "improbable" que puedan por sí mismos conllevar la inconstitucionalidad de una ley[797]. Sin embargo, los preceptos son invocables y los Jueces y Tribunales tienen que tenerlos en cuenta en todo momento a la hora de adoptar sus resoluciones[798]. El TC podrá decretar la inconstitucionalidad de una ley atendiendo a estos principios[799].

Los casos más probables en que se podría decidir la inconstitucionalidad de una norma fundamentándose directamente en los principios rectores de la política social y económica podrían ser dos, como algún autor ha apuntado con acierto: el supuesto en que la norma aprobada anula prácticamente una prestación conquistada en alguno de los ámbitos que se recogen en estos principios, sin que haya contraprestación para resarcir los daños que pueda producir; y el citado supuesto en que la norma aprobada plantea situaciones de desigualdad no-justificada afectando la situación jurídica de un grupo de ciudadanos de manera negativa e injustificada[800]. En este sentido, el propio TC ha empleado en ocasiones los principios rectores, directamente, como criterio para realizar el análisis de constitucionalidad de alguna norma[801].

Las diferentes funciones que se han citado de estos principios exigen que se les reconozca en la Constitución un contenido mínimo. Se ha apuntado que los derechos que se reconocen en el articulado del Capítulo III no contienen un "contenido esencial" deducible directamente del texto constitucional, que el legislador tenga que respetar en todo caso al desarrollar los preceptos contenidos en dicho apartado[802]. Esta conclusión se ha deducido directamente de la lectura del artículo 53 de la CE[803], que parece reconocer el contenido esencial sólo en los derechos y libertades recogidos en el Capítulo segundo. Sin embargo, dicha interpretación negando la existencia de ese contenido mínimo identificable en la propia Constitución para los principios rectores ha sido cuestionada por parte de la doctrina[804].

La existencia de un contenido esencial en el sentido que plantea la denominada teoría absoluta, que parece haber sido aceptada por la jurisprudencia y según la cual se puede delimitar

[796] PÉREZ ROYO, *Curso de Derecho...*, cit., 1997, p. 359; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 63-63; DIEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 66.
[797] STC 20 de febrero de 1989, FJ 4.
[798] PRIETO SANCHIS, *Estudios sobre Derechos...*, cit., 1990, pp. 193-194; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 56-57; PRADA FERNÁNDEZ DE SANMAMED, "Revisión de los principios…", cit., 2003, p. 294; DIEZ PICAZO, *Sistema de...*, cit., 2005, p. 66.
[799] GARCÍA de ENTERRÍA, *La Constitución...*, cit., 2006, pp. 75-76; LASAGABASTER HERRARTE, *Fuentes del Derecho…,* cit., 2007, p. 41.
[800] COBREROS MENDAZONA, *Los Tratamientos...*, cit., 1988, pp. p. 176. STC 6 de julio de 1987, FJ 3.
[801] SSTC 18 de julio de 1989, FJ 10 y 10 de febrero de 1992, FFJJ 11 y 12.
[802] STC 18 de julio de 1989, FJ 10.
[803] GONZÁLEZ MORENO, *El Estado...*, cit., 2002, p. 128
[804] GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 183-184; GARCÍA MACHO, "Los Derechos Fundamentales Sociales…", cit., 2009, p. 78.

una esfera inamovible que constituye un núcleo al que el legislador no puede afectar, es discutible. Realmente, lo que se debate en este momento es si de la redacción de la Constitución se desprende un contenido mínimo de estos principios, no ya que sea inaccesible para el legislador, sino que sirva para llevar a cabo ejercicios de ponderación entre estos principios y otros bienes jurídicos reconocidos también en la norma suprema.

Si se aceptara la idea de que no existe dicho contenido a respetar, que se desprende directamente del articulado de la Constitución, podría llegarse a la conclusión de que el legislador dispone de total libertad a la hora de regular estos aspectos. Lógicamente esta afirmación no tiene razón de ser[805]. De la cláusula del Estado social, y en concreto de los principios de igualdad material y de libertad, deriva la obligación de los poderes públicos de garantizar unos mínimos de calidad en todos los aspectos que este apartado de la Constitución reconoce.

Es cierto que a falta de desarrollo legal de estos preceptos es realmente complicado determinar un contenido mínimo que invocar. Además, la fijación de ese mínimo dependerá también de las condiciones, sobre todo, socio-económicas en cada momento histórico. Sin embargo, este problema también se da en los derechos fundamentales a la hora de determinar el contenido esencial que la propia CE reconoce. Si los poderes públicos y los ciudadanos están vinculados al contenido de la totalidad de la Constitución, al contenido de los principios rectores también, y si estos principios informan la actividad de los poderes públicos, necesariamente tiene que identificarse de la propia Constitución un contenido a estos preceptos para que estos efectos sean posibles[806]. La propia jurisprudencia ha afirmado en algún caso que estas disposiciones no pueden considerarse como normas sin contenido[807].

Si se reconoce que de dichos preceptos se deduce un contenido determinado, este contenido tendrá que ser respetado, en todo caso, por los poderes públicos, también por el legislador[808]. Al igual que ocurre con los derechos fundamentales, tendrá que identificarse caso por caso el contenido mínimo de estos principios, que en definitiva se traducirá en un mínimo de actuación a llevar a cabo por los poderes públicos para hacer efectivos los derechos reconocidos en dichos preceptos.

II.2.2. El derecho a la protección de la salud como límite al derecho fundamental a la autodeterminación informativa.

Puede parecer que hoy día el debate sobre la naturaleza jurídica del derecho a la protección de la salud carece de sentido[809]. En la medida en que el precepto constitucional que recoge este principio ha sido desarrollado por el legislador, el derecho a la protección de la salud despliega plena eficacia ante todos los poderes públicos. Se ha concretado en las leyes el contenido de este derecho reconociendo facultades concretas que son alegables y exigibles ante los

[805] GARCÍA de ENTERRÍA, *La Constitución...*, cit., 2006, p. 76.
[806] GARRIDO GUTIÉRREZ, "El Valor...", cit., 1994, p. 229; GONZÁLEZ MORENO, *El Estado...*, cit., 2002, pp. 187-194.
[807] SSTC 5 de mayo de 1982, FJ 13 y 5 de noviembre de 2007, FJ 7.
[808] STC 10 de febrero de 1992, FJ 11.
[809] BENITO, "España…", cit., 2006, p. 225.

tribunales. Sin embargo, es interesante acercarse a analizar los diferentes argumentos que se han dado para comprender mejor si este principio, por sí mismo, puede llegar a limitar un derecho fundamental.

En el contexto que se ha expuesto, y dentro del apartado dedicado a los principios rectores de la política social y económica, se ha recogido el derecho a la protección de la salud[810]. Indudablemente, el que este principio se reconozca en este apartado ha condicionado las características del mismo.

La Constitución recoge expresamente el derecho a la protección de la salud. Hay que distinguir este principio del derecho a la salud. El derecho a la protección de la salud no constituye un derecho de resultado. No es un derecho a no estar enfermo, sino, simplemente, a que los poderes públicos pongan todos los medios para que la salud de las personas sea la mejor posible[811]. De la misma forma que no se puede reconocer un derecho a la felicidad, tampoco se puede afirmar la existencia del derecho a la salud, pues la salud "es un estado de existencia, no algo que pueda ser dado"[812]. Los poderes públicos podrán o, más bien, deberán disponer los medios necesarios para que esta salud plena pueda ser alcanzada[813].

El carácter social del Estado obliga a llevar a cabo todas las acciones necesarias para que las desigualdades en el ámbito de la salud desaparezcan y todos los ciudadanos tengan garantizada una protección mínima. Se trata de hacer efectiva la igualdad real en este sector[814]. Los poderes públicos se comprometen a realizar las acciones pertinentes para prevenir los posibles problemas de salud que puedan afectar a la ciudadanía y restablecer y mantener dicho estado de salud en buenas condiciones[815].

Del precepto constitucional que reconoce el derecho a la protección de la salud se han dado diferentes interpretaciones. Hay que profundizar en la naturaleza jurídica de este derecho para entender que puede llegar a constituir un límite a un derecho fundamental. Su consideración como mero principio rector ha sido cuestionada por parte de la doctrina. Hay quien ha visto, partiendo de un concepto amplio de los derechos fundamentales[816], la posibilidad de reconocer en este principio un derecho fundamental.

Esta posición se puede basar en la especial relevancia que tiene la salud en la búsqueda del bienestar general de las personas y en la consideración de la plena integridad física y moral como pilar fundamental en la salvaguarda de la dignidad[817]. El derecho a la salud constituye un valor fundamental de esta sociedad[818.] La importancia de la salud ha sido puesta de manifiesto en numerosas ocasiones en diferentes textos de carácter internacional. La ONU, en alguno de sus

[810] Artículo 43 CE.
[811] BORRAJO DACRUZ, "Comentario al artículo...", cit., 1996, p. 183-184.
[812] PEMAN GAVIN, *Derecho a a la salud*..., cit., 1989, pp. 26-28.
[813] ESCRIBANO COLLADO, *El Derecho*..., cit., 1976, p. 45.
[814] ESCRIBANO COLLADO, *El Derecho*..., cit., 1976, pp. 11-12.
[815] RIVERO LAMAS, *Protección de la salud...,* cit., 2000, pp. 40-44.
[816] TAJADURA TEJADA, "La protección…", cit., 2004, pp. 217-218.
[817] RIVERO LAMAS, *Protección de la salud...,* cit., 2000, p. 46.
[818] ÁLVAREZ-CIENFUEGOS SUÁREZ, "La Naturaleza...", cit., 1999, p. 149-150.

informes relativos a la protección de la salud, ha reconocido que el derecho al nivel de salud más alto posible, recogido en la Declaración Universal de Derechos Humanos, constituye un "derecho humano fundamental"[819]. Así lo ha hecho también la OMS[820]. Es cierto que el sentido que en estos textos se da al concepto de "derecho humano fundamental" no es el mismo que el dado en la Constitución española a los derechos fundamentales. En el ámbito internacional la consideración de este derecho como fundamental simplemente viene a subrayar la relevancia del mismo, mientras que en el ordenamiento interno este reconocimiento conlleva efectos jurídicos de gran importancia. No obstante, estas apreciaciones dan muestra de la relevancia del derecho que ahora se comenta.

Esta interpretación podría ser compartida. Sin embargo, más allá de consideraciones en clave de *lege ferenda*, lo cierto es que la inclusión del derecho a la protección de la salud en el apartado concerniente a los principios rectores de la política social y económica hace difícil que se pueda considerar como derecho fundamental, en el sentido otorgado por la Constitución a estos últimos.

Así, en algún momento, partiendo de una visión más cercana a la letra de la Constitución, se ha argumentado incluso que el derecho a la protección de la salud no es, *per se*, un derecho subjetivo que se pueda invocar y reivindicar frente a los poderes públicos[821]. Como exige expresamente la Constitución, sólo cuando el precepto constitucional es desarrollado por el legislador puede exigir el ciudadano el respeto y la ejecución de este principio concretado en cada caso en los derechos que del desarrollo del legislador puedan derivar[822]. La CE no determina qué prestaciones y acciones componen concretamente el derecho a la protección a la salud. Es el legislador el que ha de determinar su contenido que será reivindicable ante los poderes públicos[823]. Así, el derecho a la protección de la salud, como principio rector, no sería más que una mera invitación a los poderes públicos a hacer todo lo posible para promover las condiciones necesarias para proteger la salud de las personas.

Si se admitiera esta última interpretación difícilmente podría reconocerse la posibilidad de un conflicto jurídico real entre este principio y los derechos fundamentales, a los que la Constitución otorga unas garantías máximas y una posición privilegiada en el marco jurídico. Todo conflicto se resolvería a favor de los derechos fundamentales.

Se entiende aquí, que el que no se considere el derecho a la protección de la salud un derecho fundamental no quiere decir que se erija en un mero principio sin valor jurídico, y que, en caso de conflicto con un derecho fundamental como la autodeterminación informativa, no siempre va a prevalecer este último. Hay argumentos suficientes para considerar que el principio reconocido en la Constitución constituye un derecho subjetivo. Dentro del apartado dedicado a

[819] Informe del Relator Especial, Paul Hunt, sobre el derecho de toda persona a disfrutar del nivel más alto posible de salud física y mental, presentado ante la Asamblea General el 11 de agosto de 2008.
[820] Constitución de la OMS, aprobada por la Conferencia Sanitaria Internacional, 22 de julio de 1946.
[821] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 21; GARRIDO FALLA, "Comentario al artículo 43...", cit., 2001, p. 879; SANTAMARÍA PASTOR, *Principios de derecho*..., cit., 2002, p. 204.
[822] FERNÁNDEZ PASTRANA, *El Servicio*..., cit., 1984, pp. 55-61.
[823] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 86.

los principios rectores se reconocen diferentes tipos de principios. Desde mandatos a los poderes públicos hasta derechos expresamente reconocidos. Hacer un análisis compartido para todos ellos no es acertado pues cada principio presenta sus particularidades.

Ha apuntado parte de la doctrina que parece innegable el carácter de derechos subjetivos de, cuando menos, algunos de los principios[824]. El derecho a la protección de la salud es uno de ellos, así como el derecho a disfrutar de un medioambiente adecuado[825]. De ahí que cuando se habla de este derecho se hace considerándolo como un principio "subjetivizado", por cuanto que no sólo se realiza un mandato a los poderes públicos, sino que se hace un reconocimiento expreso de un derecho[826].

Los argumentos favorables a esta interpretación son distintos. En primer lugar, el que en el enunciado constitucional se recoja este principio como "derecho" es significativo. Aunque sea indirectamente, se reconoce que las personas podrán ejercer ante los poderes públicos una serie de facultades. Si bien dispone la Constitución que de los principios no derivan directamente derechos concretos, la calificación como derecho de este precepto da a entender que de su contenido se desprenden ciertas facultades para los ciudadanos, no sólo mandatos dirigidos a los poderes públicos.

En segundo lugar, hay que tener en cuenta que el precepto que reconoce en la Constitución el derecho a la protección de la salud, a pesar de su ambigüedad, marca una serie de pautas que determinarán el contenido de dicho derecho[827]. Como se verá en el apartado siguiente, el precepto ya establece, aunque en términos generales, cuál es el ámbito que ha de abarcar el derecho. Al referirse tanto a la "salud" como a la "salud pública" reconoce que la protección se dará tanto en términos asistenciales como preventivos.

En tercer lugar, el que en los textos internacionales se reconozca expresamente el derecho a la protección de la salud como un derecho humano, incluso fundamental, hace ver que el principio que ahora se trata puede ser interpretado como derecho. La Constitución dispone que las normas que regulan los derechos fundamentales y las libertades recogidas se interpretarán de acuerdo con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España[828]. Pues bien, como se ha dicho, tanto la citada declaración[829] como el Pacto Internacional de Derechos económicos, sociales y culturales[830] reconocen el derecho a la protección de la salud y lo interpretan como un derecho humano fundamental. Y, a pesar de que el carácter fundamental tenga aquí un sentido

[824] ABRAMOVICH y COURTIS, *Los Derechos…*, cit., 2002; ÉNERIZ OLAECHEA, *La Protección…,* cit., 2007, p. 99.
[825] LOPERENA ROTA, "La protección de la salud…", cit., 1991, p. 1464; LASAGABASTER HERRARTE, GARCÍA URETA y LAZCANO BROTONS, *Derecho Ambiental…,* cit., 2007, p. 454; EMBID IRUJO, *El Derecho a un Medio Ambiente…,* cit., 2008, pp. 318-319.
[826] RODRÍGUEZ-PIÑERO y DEL REY, "Informe Español"…, cit., 1999, p. 97.
[827] BALAGUER CALLEJÓN, *Derecho Constitucional*..., cit., 2003, p. 257.
[828] Artículo 10.2 CE. IBÁÑEZ MÉNDEZ, "Los Poderes Públicos…", cit., 2003, p. 55.
[829] Artículo 25 Declaración Universal de Derechos Humanos, 1948.
[830] Artículo 12 Pacto Internacional de Derechos económicos, sociales y culturales, 1966.

distinto al que se le confiere en el ordenamiento interno, su reconocimiento como tal hace difícil que la protección de la salud no se considere, cuando menos, como derecho.

Por último, basta con remitirse a los diferentes pronunciamientos que Jueces y Tribunales han realizado en aplicación del artículo 43 de la Constitución para darse cuenta, como no podía ser de otra manera, que de dicho precepto deriva un derecho subjetivo a todos los efectos. El reconocimiento a una persona del derecho a una indemnización por la actuación negligente de un profesional sanitario, fundamentándose en la vulneración del citado precepto constitucional es significativo en este sentido[831]. Incluso se ha llegado a considerar este principio como derecho fundamental por los tribunales, si bien es cierto que lo han hecho poniéndolo en relación con el derecho fundamental a la integridad física[832]. Dependiendo del caso los tribunales inciden en el carácter de principio rector del derecho a la protección de la salud o en su carácter de derecho subjetivo, aunque parece primar la interpretación de que el principio del que se habla no tiene otra naturaleza jurídica que la de derecho subjetivo. Esta solución se deduce también, quizás con menos claridad, cuando lo que se sanciona no es una acción negligente del profesional sanitario, sino la omisión de socorro por parte de éste a una persona que lo necesita, provocándole un riesgo grave para su salud. El Código Penal castiga esta actitud[833]. Se puede interpretar que si las leyes sancionan este hecho lo hacen porque se entiende que la persona que sufre esta omisión tiene derecho a que su salud se proteja en cierta medida. ¿Cabría pensar que si el artículo 43 CE no tuviera desarrollo legal, esta actitud omisiva no sería sancionable? No parece que esta solución sea asumible, de lo que necesariamente ha de reconocerse un contenido mínimo a dicho precepto constitucional.

También puede argumentarse como punto de apoyo de esta tesis el que de la jurisprudencia del TEDH se desprenda la aplicabilidad directa de este principio como derecho. En más de una ocasión se ha basado este Tribunal en el derecho a la salud, encauzado o integrado en el derecho a la vida privada[834], para limitar las actuaciones de otros agentes. Como bien ha señalado la doctrina, si en el ámbito de este Tribunal puede invocarse este derecho de manera directa, por qué no admitir esta posibilidad en el ordenamiento interno[835]. Si bien es cierto que la Constitución no caracteriza los principios rectores de la política social y económica como derechos directamente alegables ante los Tribunales, tampoco afirma lo contrario, por lo que no impide que en la práctica sean tratados como tales.

Partiendo de estas consideraciones se le puede otorgar al derecho a la protección de la salud entidad suficiente como para constituirse en límite de derechos fundamentales. Esta afirmación puede basarse en los siguientes argumentos.

---

[831] SAP de Cantabria 25 de noviembre de 1993, FJ 2. PEMÁN GAVÍN, *Derecho a la salud…,* cit., 1989, p. 95.
[832] STSJ de Galicia de 30 de abril de 1997.
[833] Artículo 196 CP: "*El profesional que, estando obligado a ello, denegare asistencia sanitaria o abandonare los servicios sanitarios, cuando de la denegación o abandono se derive riesgo grave para la salud de las personas, será castigado con las penas del artículo precedente en su mitad superior y con la de inhabilitación especial para empleo o cargo público, profesión u oficio, por tiempo de seis meses a tres años*"; STS 28 de enero de 2008.
[834] Artículo 8 CEDH. SSTEDH 9 de diciembre de 1994, López Ostra v. España; 10 de noviembre de 2004, Taskin y otros v. Turquía; 26 de octubre de 2006, Ledyayeva y otros v. Rusia.
[835] LASAGABASTER HERRARTE, GARCÍA URETA y LAZACANO BROTONS, *Derecho Ambiental…,* cit., 2007, p. 460.

Cuando se habla de limitar un derecho fundamental son muchas las interrogantes que se plantean. La distinción entre delimitación y limitación, la existencia o no de un contenido esencial de dichos derechos, la clasificación de los límites, etc. No se pretende en este momento hacer un estudio sobre estos extremos, pues sobrepasaría la intención de este trabajo y se desviaría la atención hacia cuestiones teóricas cuyo análisis no procede en este momento. Basta, para el fin que se pretende, analizar si es posible realizar un juicio ponderativo entre los dos bienes jurídicos que entran en juego ahora: el derecho a la protección de la salud y el derecho fundamental a la autodeterminación informativa. Se trata de ver si el derecho a la protección de la salud puede, desde la perspectiva constitucional, constituir un bien jurídico suficiente para limitar el derecho a la autodeterminación informativa.

Como se ha puesto de manifiesto en innumerables ocasiones tanto por la doctrina como por la jurisprudencia los derechos fundamentales no son absolutos[836]. Concretamente, en referencia al derecho fundamental que aquí se estudia el TC se ha pronunciado refrendando esta afirmación[837]. Los derechos fundamentales en primer lugar se delimitan. La delimitación ha sido definida por parte de la doctrina como sinónimo de conformación, como "la determinación de los linderos conceptuales del derecho (...) o cualquier otra actuación dirigida a proteger, promover, posibilitar o facilitar el ejercicio de un derecho fundamental y *que no tenga ningún contenido gravoso o restrictivo sobre el derecho para los titulares de que se trate*"[838]. Supone la concreción del contenido de cada derecho. Una vez delimitados, pueden encontrarse límites a estos derechos en la medida en que colisionan con otros bienes jurídicos. Los límites constituyen restricciones al derecho delimitado, configurado, cuyos contornos han sido definidos. En ocasiones la delimitación y la fijación de los límites a estos derechos se realiza de manera meridianamente clara en la propia Constitución[839]. Sin embargo, la mayoría de veces estas excepciones hay que deducirlas del ordenamiento. En relación con la mayoría de los derechos la CE se limita a realizar una mención genérica sobre la mera existencia del derecho fundamental.

Ante la vaguedad de los preceptos que se refieren a los derechos fundamentales la actuación del legislador se erige en fundamental para concretar su contenido constitucional y sus límites[840]. La necesidad de que los ciudadanos conozcan el alcance de los derechos, la seguridad jurídica exige, sobre todo, que los límites de los mismos sean definidos. Esta actividad de concretización no se trata, sin embargo, de una actuación meramente automática, sino que conlleva también un ejercicio creativo, fundamentalmente de interpretación[841]. Los amplios márgenes que la Constitución deja para la discrecionalidad del legislador son ya conocidos. En un Estado que proclama el pluralismo político como uno de sus valores superiores la Constitución ha de dejar

[836] GÓMEZ SÁNCHEZ, *Derechos y Libertades…,* cit., 2003, p. 79; NARANJO DE LA CRUZ, *Los límites…,* cit., 2000, pp. 73-74; BRAGE CAMAZANO, *Los límites...,* cit., 2004, p. 35. STC 22 de marzo de 1991, FJ 2; STS 22 de julio de 2008, FJ 4.
[837] STC 30 de noviembre de 2000, FJ 11.
[838] NARANJO DE LA CRUZ, *Los límites…,* cit., 2000, p. 72.
[839] Artículo 20.4 CE: *"Estas libertades (*de expresión y de información*) tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia*".
[840] MEDINA GUERRERO, *La Vinculación*..., cit., 1996, pp. 23-25; UGARTEMENDIA ECEIZABARRENA, *El Derecho*..., cit., 2001, pp. 28-29; BRAGE CAMAZANO, *Los Límites*..., cit., 2004, p. 88.
[841] MEDINA GUERRERO, *La Vinculación…*, cit., 1996, p. 25.

margen para que en cada momento histórico puedan llevarse a cabo diferentes formas de interpretación de los preceptos constitucionales en general, y de los derechos fundamentales en particular. En el caso del derecho a la autodeterminación informativa el artículo 18.4 de la Constitución no recoge expresamente límite alguno, simplemente invita al legislador a limitar el uso de la informática. Es por ello que será el legislador, y el TC en el ejercicio de control de constitucionalidad de las leyes, el que realizando la citada labor interpretativa, deberá deducir de la Constitución los límites del derecho a la autodeterminación informativa[842].

La interpretación que debe llevar a cabo el legislador tiene que resultar de la aplicación del principio de proporcionalidad cada vez que diferentes bienes jurídicos chocan entre sí. Se trata de ponderar los valores en juego para ver en qué medida se limita uno de ellos en beneficio del otro, de buscar el equilibrio entre los bienes jurídicos que colisionan[843]. Cabe preguntarse en este momento si resulta proporcional limitar un derecho fundamental para favorecer la realización efectiva de un bien jurídico que es considerado en la Constitución como un principio rector de la política social y económica.

Desde una interpretación reduccionista podría entenderse que las diferencias que se marcan en la Constitución, desde el punto de vista de las garantías jurídicas, entre derechos fundamentales y principios rectores llevan a considerar estos últimos como valores de inferior categoría que los primeros. Este análisis podría llevar a la conclusión de que no es acorde al principio de proporcionalidad limitar el derecho fundamental a la autodeterminación informativa con el fin de favorecer el derecho a la protección de la salud. Nada más lejos de la realidad.

En primer lugar, se ha dicho que el derecho a la protección de la salud puede reivindicarse ante los Jueces y Tribunales mediante otros derechos fundamentales, especialmente a través de los derechos a la vida y a la integridad física y moral. En estos supuestos no habría duda alguna sobre la posibilidad de alegar el derecho a la protección de la salud frente al derecho fundamental que se comenta, pues la ponderación se realizaría entre bienes jurídicos de la misma consideración constitucional[844].

Desde una segunda perspectiva la solución ha de ser la misma. Si se toma el derecho a la protección de la salud de manera independiente, sin ponerlo en relación con otros derechos fundamentales, también ha de ser alegable en el momento en que colisiona con un derecho fundamental. Los argumentos para apoyar esta afirmación ya han sido citados.

A la hora de realizar la labor interpretativa, que llevará al legislador a deducir los límites del derecho fundamental a la autodeterminación informativa, deberá basarse en bienes jurídicos recogidos en la Constitución[845]. Ha habido unanimidad entre doctrina y tribunales para afirmar que la norma suprema debe interpretarse como una unidad que ha de tenerse en cuenta en su conjunto[846]. Se trata de buscar el equilibrio entre todos los derechos y principios reconocidos en

[842] MUÑOZ ARNAU, *Los Límites*..., cit., 1998, p. 105.
[843] SSTC 17 de julio de 1986, FFJJ 5 y 6; 18 de julio del 2002, FFJJ 12 y 13;
[844] STC 25 de marzo de 1996.
[845] BRAGE CAMAZANO, *Los límites...,* cit., 2004, p. 83.
[846] SSTC, 4 de febrero de 1984, FJ 3; 11 de diciembre de 1987, FJ 7.

la misma[847]. En este sentido, el TC ha afirmado que hay que buscar la convivencia entre todos estos bienes, de tal forma que un derecho no pueda imponerse a los demás de manera ilimitada. La ponderación no se realiza sólo entre los derechos fundamentales, sino entre todos los derechos y valores reconocidos en la Constitución. El TC en este sentido ha entrado a analizar el enfrentamiento entre un derecho fundamental y el interés general que resulta de un bien jurídico que formalmente no constituye un derecho fundamental, como es la obligación de todos de sostener los gastos públicos[848]. De esta jurisprudencia es deducible que cuando diferentes bienes jurídicos chocan, lo relevante no es su consideración en la Constitución como derecho fundamental o como principio rector, sino la correcta aplicación del principio de proporcionalidad entre los bienes que colisionan.

El derecho a la protección de la salud, tal y como está recogido en la Constitución, presenta características que lo hacen susceptible de ser ponderado cuando entra en colisión con otros bienes jurídicos. Ya se ha apuntado más arriba que de este precepto resulta un contenido mínimo a tener en cuenta por el legislador en todo caso. Se hacía referencia al hecho de que el derecho a la protección de la salud ha de contener medidas dirigidas a promover la salud tanto desde el punto de vista asistencial como preventivo. Ya se ha argumentado la consideración de este derecho como derecho subjetivo de especial vinculación con la dignidad de las personas. La relevancia que se ha otorgado en este trabajo al derecho a la protección de la salud despeja toda duda que se pueda plantear sobre su aplicabilidad como límite de los derechos fundamentales.

En lo que aquí concierne, la manipulación de datos de carácter personal sanitarios es indispensable para la efectiva salvaguarda de la salud de las personas. En ocasiones, el tratamiento de esta información se podrá llevar a cabo con el consentimiento del titular de los datos. Sin embargo, como se verá, la necesidad de requerir esta autorización puede muchas veces entorpecer y ralentizar la labor sanitaria. Puede plantearse, por lo tanto, que la protección de la salud constituye un límite al derecho fundamental a la autodeterminación informativa. La resolución del choque entre estos bienes vendrá de la aplicación del principio de proporcionalidad. Como se verá más adelante, la LOPD ya ha dado, aunque no de forma especialmente clara, solución a esta confrontación. En la Ley se ha reconocido que la protección de la salud puede ser un límite al derecho fundamental a la autodeterminación informativa. Si se interpreta que la protección de la salud constituye un bien jurídico suficiente para limitar el derecho fundamental a la autodeterminación informativa, interesa delimitar el ámbito de realidad que abraza la protección de la salud. Esta delimitación llevará a determinar hasta dónde llega el límite al derecho fundamental a la autodeterminación informativa que se analiza.

II.2.3. El ámbito de realidad salvaguardado por el derecho a la protección de la salud.

II.2.3.A. La necesidad de entender el derecho a la protección de la salud en sentido amplio.

La importancia de delimitar el ámbito que abraza el concepto de salud en el ordenamiento es grande. Ese ámbito será la base de una posible excepción al derecho fundamental a la

[847] STC 8 de abril de 1981, FJ 7.
[848] STC 23 de febrero de 1995, FJ 6.

autodeterminación informativa. La jurisprudencia ha reconocido en algún caso de manera expresa la relevancia de dar esta definición, si bien refiriéndose a la necesidad de delimitar el concepto de "dato relativo a la salud"[849]. Ya se ha dicho que el considerar una información como relativa a la salud de las personas la convierte en información especialmente protegida por la Ley.

Dar una definición del concepto salud es una tarea compleja, fundamentalmente porque se está haciendo referencia a una realidad que va cambiando con el tiempo[850] y que puede ir abrazando cada vez diferentes circunstancias o situaciones[851]. Lo que antes se podía considerar como enfermedad ahora no se considera como tal y al revés, van apareciendo nuevas afecciones o dolencias. Se trata de un concepto que está muy abierto a diferentes interpretaciones[852].

Hay que tener en cuenta además que la protección de la salud requiere de actuaciones que afectan a otros derechos, libertades o bienes jurídicos que tienen que ser considerados, a saber: el derecho a la vida, a la libertad entendida en sentido estricto, el derecho al honor, incluso el derecho a una vivienda digna o al trabajo y como no, el derecho a la autodeterminación informativa[853]. Esta idea aparece plasmada en la conclusión que muchos autores recogen de que el derecho a la protección de la salud aparece, aunque sea implícitamente, reconocido en otros muchos preceptos de la propia Constitución que se dirigen, en principio, a regular otros aspectos de la vida[854]. Especial relación se da entre el derecho a la protección de la salud y la regulación de un sistema de Seguridad Social al que se refiere la CE en el artículo 41, pues ambas figuras se refieren a ámbitos o campos que en algunas ocasiones coinciden[855]. Lo mismo ocurre con la obligación de los poderes públicos de llevar a cabo acciones sociales a favor de las personas disminuidas físicas, sensoriales y psíquicas[856], o con la obligación de promover la investigación científica en beneficio del interés general[857].

No se quiere en este momento profundizar en el debate sobre lo que hay que entender por "salud", pues se trata de un concepto que requiere de un análisis complejo y lleno de matices[858]. Bastará con señalar las conclusiones fundamentales que se han extraído de dicho debate con el fin de determinar cuál es el ámbito al que se hace referencia cuando se habla del tratamiento de datos con la finalidad de proteger la salud.

[849] STSJ de Asturias 12 de septiembre de 2005, FJ 14.
[850] NAVARRO LÓPEZ, "Concepto Actual...", cit., 1998, pp. 51-52; MARTÍNEZ HERNÁNDEZ, *Nociones de Salud…,* cit., 2003, pp. 9-10.
[851] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 28; CURREA-LUGO, *La Salud*..., cit., 2005, p. 74.
[852] NAVARRO LÓPEZ, "Concepto Actual...", cit., 1998, pp. 49-50.
[853] CURREA-LUGO, *La Salud*..., cit., 2005, p. 13.
[854] BORRAJO DACRUZ, "Comentario al artículo...", cit., 1996, pp. 169-170; GONZÁLEZ MORENO, *El Estado Social*..., cit., 2002, pp. 212-213.
[855] BORRAJO DACRUZ, "Comentario al artículo...", cit., 1996, pp. 180-181.
[856] Artículo 49 CE.
[857] Artículo 44.2 CE.
[858] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 31; BORRAJO DACRUZ, "Comentario al artículo...", cit., , 1996, p. 168.

Desde la doctrina se han dado diferentes interpretaciones del concepto al que se está haciendo referencia[859]. Interesa aquí poner de manifiesto una restrictiva y otra más amplia. Desde la primera perspectiva se ha planteado que el derecho a proteger la salud es la facultad de exigir al Estado una acción dirigida a proteger la salud individual de cada uno[860]. Desde otro punto de vista, más amplio, este derecho constituiría la posibilidad de exigir al Estado la promoción de las condiciones necesarias para garantizar una vida digna[861].

Como se ve, la primera definición, anterior a la aprobación de la Constitución, es ejemplo de una visión restrictiva de lo que se entiende por derecho a la protección de la salud. Es el reflejo de una forma de interpretarlo desde la perspectiva exclusivamente individual, refiriéndose a medidas que tienen por objeto el individuo y no la colectividad. En cambio, la segunda definición, más actual, parece afectar a todo tipo de medidas que garanticen la salud de las personas. Se hace referencia incluso a la salud como medio para garantizar una vida digna, lo cual parece dar pie a que dentro de estas medidas se encuentren algunas, que sin ser estrictamente de carácter médico afectan de alguna manera a la salud de las personas.

A lo largo de la historia, el concepto de derecho a la protección de la salud ha ido cambiando constantemente de contenido[862]. Sin embargo, hoy día parece que hay acuerdo en asumir la interpretación amplia, considerando que se trata de un derecho que afecta a aspectos de la vida muy diferentes y a intereses muy diversos[863]. La ubicación del individuo dentro de una colectividad lleva a pensar que la salud de la persona no depende sólo de factores personales sino también de factores externos[864]. En la salud de cada persona no sólo inciden aspectos individuales, físicos y mentales, sino también circunstancias colectivas del entorno social que afectan a la salud de la persona[865]. Por eso, la protección de la salud engloba acciones dirigidas a proteger tanto la salud del individuo como la salud colectiva[866]. La relevancia de la salvaguarda de la salud pública es un hecho contrastado. Se entiende por salud pública "la ciencia y el arte de mejorar la salud de la población mediante los esfuerzos organizados de la sociedad, usando las

[859] DELGADO RODRÍGUEZ y LLORCA DÍAZ, "Concepto de Salud…", cit., 2008, p. 3.

[860] ESCRIBANO COLLADO, *El Derecho*..., cit., 1976, pp. 44-45: se trata de "aquel derecho individual que se ostenta frente al Estado a fin de obtener una acción positiva de éste dirigida a la efectiva satisfacción de la salud individual por encima de las posibilidades personales del sujeto".

[861] CURREA-LUGO, *La Salud*..., cit., 2005, p. 38: se ha entendido que el derecho a protección de la salud "tiene su materialización en la exigencia de medios que garanticen y/o restablezcan unas condiciones adecuadas de la naturaleza biológica de la persona, pero no toda su naturaleza sino de aquella alterada, que llamamos enfermedad, y para la cual la ciencia nos ofrece posibilidades".

"La exigencia buscada no es sólo en materia de supervivencia (urgencias, por ejemplo) sino también en términos de la salud como medio para garantizar una vida digna. Si sólo fuera invocable la salud como derecho cuando hay riesgo para la vida, se limitaría toda reclamación de salud al dilema vida o muerte, con lo que el reconocimiento de la salud quedaría subsumido por el derecho a la vida".

p. 72: "una equilibrada y adecuada condición dinámica de la naturaleza biológica de la persona, objetivamente comprobable, moralmente aceptable (en cuanto socialmente consensuada), que se podría mantener bajo ciertas condiciones, vulnerable a ciertos factores, y potencialmente garantizable y/o recuperable mediante el uso de una determinada técnica, y, en cuanto tal, exigible jurídicamente".

[862] MARSET CAMPOS y SÁEZ GÓMEZ, "La Evolución...", cit., 1998, pp. 1-22.

[863] PEMÁN GAVÍN, *Derecho a la Salud...,* cit., 1989, p. 88; ÁLVAREZ-CIENFUEGOS SUÁREZ, "La Naturaleza...", cit., 1999, p. 154.

[864] VAQUERO PUERTA, *Salud Pública*…, cit., 1988, p. 24.

[865] CASTELLANOS, "Los Modelos...", cit., 1998, pp. 81-102.

[866] ESCRIBANO COLLADO, *El Derecho*..., cit., 1976, p. 11; NICOLÁS ORTIZ, *El Derecho*..., cit., 1983, pp. 31-34.

técnicas de prevención de la enfermedad y de protección y promoción de la salud"[867]. La salud pública engloba acciones de vigilancia, de identificación de políticas efectivas que mejoran la salud a través de la investigación, la implantación de estas estrategias, la gestión de programas de prevención, la provisión de servicios sanitarios suficientes y evaluación de las estrategias seguidas[868].

La protección de la salud, sobre todo desde esta perspectiva colectiva, tiene en cuenta todos los aspectos que interfieren en la salud de las personas. Piénsese en el ocio, el trabajo, el medioambiente, la alimentación, etc[869]. Necesariamente, la protección de la salud ha de incluir acciones que tengan en cuenta estas cuestiones. Hoy día parece indudable la influencia del estado del medioambiente en la salud de las personas. Se habla de conceptos como "salud ambiental" o "epidemiología ambiental", que ponen en relación las dos realidades[870]. Que las condiciones de trabajo tienen influencia directa sobre la salud de las personas tampoco es discutible[871]. Lo mismo ocurre con la alimentación o con el ocio[872].

En conclusión, hoy, prácticamente la totalidad de la doctrina ha coincidido en afirmar que el concepto de salud se refiere a un campo de actuación especialmente amplio que afecta a diferentes aspectos de la vida[873]. Incluso podría considerarse la salud, la buena salud física y mental, como un todo equiparable al bienestar general, o a tener unas buenas condiciones de vida. Más allá de la interpretación reduccionista de que el derecho a la protección de la salud constituye una realidad que abraza simplemente la asistencia en centros hospitalarios[874], se asume que este derecho abarca algo más que las acciones estrictamente curativas[875].

La consideración de este derecho desde esta perspectiva amplia ha sido acogida en el ámbito internacional en diferentes textos jurídicos[876]. En la Declaración Universal de Derechos Humanos se recogen en el mismo precepto el derecho de todos a la salud y al bienestar, a la alimentación, al vestido, a la vivienda a la asistencia médica y a los servicios sociales necesarios, así como a los seguros en caso de desempleo, enfermedad, invalidez, viudez, vejez u otra circunstancia en que la persona haya perdido sus medios de subsistencia[877]. Se deja entrever que se asume una interpretación especialmente amplia del concepto. Así se deduce también de

[867] MARTÍNEZ HERNÁNDEZ, *Nociones de Salud…,* cit., 2003, p. 10; HERNÁNDEZ-AGUADO, LUMBRERAS LACARRA Y GARCÍA DE LA HERA, "Concepto y Funciones…", cit., 2008, p. 7.
[868] HERNÁNDEZ-AGUADO, LUMBRERAS LACARRA Y GARCÍA DE LA HERA, "Concepto y Funciones…", cit., 2008, pp. 8 y 9.
[869] VAQUERO PUERTA, *Salud Pública*..., cit., 1988, p. 57; CURREA-LUGO, *La Salud*..., cit., 2005, pp. 29-30.
[870] BALLESTER DÍEZ y VALCÁRCEL RIVERA, "Epidemiología ambiental…", cit., 2008, p. 147.
[871] GARCÍA GARCÍA, "Problemas de salud…", cit., 2008, p. 159; VITALLER BURILLO, "Prevención en salud…", cit., 2008, p. 167.
[872] MARTÍNEZ HERNÁNDEZ, ASTIASARÁN ANCHÍA y MADRIGAL FRITSCH, *Alimentación y Salud…,* cit., 2001; VIOQUE LÓPEZ y BOLUMAR MONTRULL, "Nutrición y Salud…", cit., 2008, p. 119.
[873] CURREA-LUGO, *La Salud*..., cit., 2005, pp. 75-76.
[874] CURREA-LUGO, *La Salud*..., cit., 2005, pp. 75-76, menciona esta acepción del derecho a la protección de la salud que podría haber sido adoptada por alguna organización como el Comité de derechos económicos, sociales y culturales de las Naciones Unidas.
[875] CURREA-LUGO, *La Salud*..., cit., 2005, p. 71.
[876] MARTÍNEZ y HERNÁNDEZ, GARCÍA PERUELLES, BARÓN CRESPO, *Tratado del Derecho…*, cit., 2004, p. 121.
[877] Artículo 25.1, Declaración Universal de los Derechos Humanos de 10 de diciembre de 1948.

otros textos de la ONU, que tras reconocer la complejidad de la tarea de dar una definición a este concepto relacionan la salud con otros campos como la higiene, la alimentación o el medioambiente[878]. En lo que se llama en este organismo internacional el "derecho al disfrute del más alto nivel posible de salud física y mental", se equiparan la salud y el bienestar físico y mental[879].

En el mismo ámbito, el Pacto Internacional de Derechos Económicos, Sociales y Culturales, relaciona expresamente la protección de la salud con la garantía de un medioambiente adecuado, una vivienda digna o la higiene en el ámbito laboral, además de con una acción eficiente en materia de prevención y salud colectiva[880]. Se concluye que el derecho a proteger la salud va más allá que la mera asistencia sanitaria, incluyendo acciones de carácter preventivo y actuaciones dirigidas a garantizar una vivienda digna, un medioambiente adecuado o la salud laboral[881].

Lo mismo se hace en la OMS. En su Constitución se entiende que la salud no es otra cosa que el "bienestar físico, mental y social" y no sólo la ausencia de enfermedades[882]. En este sentido, en diferentes documentos elaborados por este organismo se subraya la relación entre la salud, entendida en sentido estricto, y otros factores[883].

En el ámbito de la UE la relación entre la salud en sentido estricto, el medioambiente, la salud colectiva o la seguridad laboral, se pone de manifiesto en múltiples textos que vinculan todas estas realidades[884]. El Tribunal de Estrasburgo, en su jurisprudencia, también ha dejado entrever una interpretación amplia de lo que puede entenderse por salud. Este tribunal reconoce el derecho a la protección de la salud vinculándolo con el derecho a la vida privada[885]. En diferentes ocasiones ha establecido la relación entre la salud, el medioambiente y conceptos más genéricos como el de bienestar o la calidad de vida[886]. El TJUE también ha tomado en consideración en

[878] Informe del Relator Especial sobre el derecho de toda persona al disfrute del nivel más alto posible de salud física y mental, presentado ante la Asamblea General el 11 de agosto de 2008; Informe del Relator Especial sobre el derecho de toda persona al disfrute del nivel más alto posible de salud física y mental, presentado ante la Asamblea General el 12 de septiembre de 2005.

[879] Resolución aprobada por la Asamblea General de la ONU, 10 de marzo de 2004.

[880] Artículo 12, Pacto Internacional de Derechos Económicos, Sociales y Culturales, 16 de diciembre de 1966.

[881] Observación General al artículo 12 del Pacto Internacional de Derechos Económicos, Sociales y Culturales, nº 14, del 11 de agosto del 2000.

[882] Constitución de la OMS, adoptada por la Conferencia Sanitaria Internacional, 22 de julio de 1946.

[883] Carta de Ottawa, emitida en la Primera Conferencia Internacional para la Promoción de la Salud, 21 de noviembre de 1986; Carta de Bangkok, emitida en la Sexta Conferencia Internacional para la Promoción de la Salud, 11 de agosto de 2005.

[884] Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo, Estrategia europea de medio ambiente y salud, COM (2003)338 final, 11 de junio de 2003; MARTÍNEZ y HERNÁNDEZ, GARCÍA PERUELLES, BARÓN CRESPO, *Tratado del Derecho…*, cit., 2004, p. 208.

[885] Artículo 8, CEDH: "*1. Toda persona tiene el derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia; 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*"; ARZOZ SANTISTEBAN, "Artículo 8, CEDH…", cit., 2004, pp. 277-280.

[886] SSTEDH 2 de noviembre de 2006, Giacomelli v. Italia; 16 de noviembre de 2004, Moreno Gómez v. España; 19 de febrero de 1998, Guerra y otros v. Italia; 9 de diciembre de 1994, López Ostra v. España; 21 de febrero de 1990, Poweel y Rayner v. Reino Unido;.

muchas ocasiones la relación entre la salud y otras esferas de la realidad como el medioambiente[887] o la seguridad alimentaria[888].

En el ámbito interno la Constitución, en su artículo 43, da pie para que pueda realizarse esa interpretación amplia del derecho que ahora se comenta. Esta norma emplea dos conceptos de relevancia: "*salud*"[889] y "*salud pública*"[890]. Podría pensarse que se refieren a realidades diferentes. La salud, frente al concepto de salud pública, parece abrazar acciones de alcance individual, principalmente de carácter asistencial. El concepto de salud pública, por el contrario, se refiere a acciones de alcance global dirigidas a proteger y promocionar la salud del colectivo, de la sociedad en general, principalmente acciones de carácter preventivo[891]. Sin embargo, lo cierto es que en la redacción de la Constitución cualquiera de los dos conceptos podría abrazar las dos realidades, tanto la de alcance individual como de carácter general. En primer lugar, porque las acciones dirigidas a salvaguardar la salud colectiva afectan en última instancia a la salud individual[892]. La protección de la salud necesariamente tiene que contemplar las acciones de carácter colectivo, que van a afectar en última instancia a la salud de los individuos. Y, en segundo lugar, porque el concepto de salud pública puede ser entendido en sentido amplio, de tal manera que englobe acciones de carácter global y particular[893]. La propia CE en el apartado que se refiere a la salud pública hace mención no sólo a medidas preventivas sino también a "*prestaciones y servicios necesarios*", lo cual deja la puerta abierta para aceptar la acepción amplia del concepto[894].

De la redacción de la Constitución claramente se deduce, por lo tanto, que la protección de la salud reclama de los poderes públicos acciones más allá de las estrictamente asistenciales. Exige no sólo actividades curativas o asistenciales que se ejercen frente al individuo, sino también medidas preventivas que, en la mayoría de los casos, suelen tener por objeto la sociedad y que persiguen que el ciudadano pueda llevar a cabo una vida "saludable"[895].

La actividad asistencial engloba necesariamente tanto la atención primaria como la secundaria o especializada[896]. Determinar las actividades concretas que los poderes públicos han de garantizar en cada uno de estos estadios dependerá sobre todo de cuestiones políticas e incluso científicas o médicas, sin embargo, es innegable que hoy en día los poderes públicos garantizan en el Estado múltiples servicios o prestaciones.

[887] STSJCE 24 de junio de 2008, Commune de Mesquer v. Total France S.A. y otros, asunto C-188/07.
[888] STSJCE 15 de julio de 2004, Douwe Egbert NV y otros v. otros y otros, asunto C-239/02.
[889] Artículo 43.1 CE.
[890] Artículo 43.2 CE.
[891] BORRAJO DACRUZ, "Comentario al artículo...", cit., 1996, pp. 188-189.
[892] CIERCO SEIRA, *Administración Pública…,* cit., 2006, p. 8.
[893] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 68; ÁLVAREZ-CIENFUEGOS SUÁREZ, "La Naturaleza...", cit., 1999, pp. 160-161; VAQUERO PUERTA, *Salud Pública*..., cit., 1988, pp. 24-25.
[894] COBREROS MENDAZONA, *Los Tratamientos*..., cit., 1988, p. 203.
[895] COBREROS MENDAZONA, *Los Tratamientos*..., cit., 1988, p. 200: p. 202; MARSET CAMPOS y SÁEZ GÓMEZ, "La Evolución...", 1998, pp. 21-22; MARTÍNEZ y HERNÁNDEZ, GARCÍA PERUELLES, BARÓN CRESPO, *Tratado del Derecho*…, cit., 2004, p. 521.
[896] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 31

Por su parte, las medidas preventivas abrazan acciones de muy diferente tipo, desde la investigación científica y realización de estudios epidemiológicos, de los que se pueden extraer conclusiones sobre las características de determinadas enfermedades para aprender a prevenirlas, hasta acciones dirigidas a mejorar la salubridad en la alimentación, en el medio ambiente, en las aguas, pasando por campañas de vacunaciones, etc.[897] La acción preventiva ha sido clasificada por algún autor en diferentes fases, en las que se engloban distintas acciones a llevar a cabo. Así, la Intervención Preventiva Primaria que se ejerce sobre factores que pueden hacer que una enfermedad aparezca; la Intervención Preventiva Secundaria que se ejerce en la fase presintomática de la enfermedad; y la Intervención Preventiva Terciaria que se lleva a cabo una vez el sujeto está ya enfermo para que los daños sean menores y así se cure y rehabilite[898]. Evidentemente, la acción preventiva por excelencia es la primaria que se ejerce sobre el colectivo o conjunto de la sociedad y que abraza actuaciones de alcance general como las citadas de limpieza de aguas, seguridad alimentaria o en los medicamentos, educación sanitaria, etc.[899].

Con los argumentos expuestos es fácil deducir que el concepto de salud que se manejará en este trabajo deberá interpretarse en sentido amplio. Es necesario, sin embargo, concretar ahora qué acciones completan o componen en la normativa sanitaria la finalidad genérica de proteger la salud[900].

II.2.3.B. La determinación en la normativa sanitaria de lo que se ha de entender por “salud”.

La concreción de lo que ha de entenderse por la protección de la salud se lleva a cabo en el ordenamiento por diferentes normas. Si se tiene en cuenta que a la salud de las personas afectan factores que tienen que ver con muy distintos y numerosos sectores de la vida se comprenderá, que es tarea prácticamente imposible enumerar todas las normas que de manera directa o indirecta regulan este sector. Interesa traer aquí la normativa que directamente regula la materia sanitaria y que delimita con exactitud los elementos que componen la protección de la salud desde una perspectiva amplia. El análisis que se realiza se centra en la manipulación de datos en el ámbito estrictamente sanitario, por lo que el estudio de otras esferas como la medioambiental o la relativa a la seguridad laboral exceden del objetivo de este trabajo.

La norma principal que determinará el ámbito de protección que abraza el derecho a la salvaguarda de la salud es la LGS. Esta Ley se erige en el desarrollo directo del precepto constitucional que reconoce el derecho a la protección de la salud[901]. Como tal, entra a concretar las actividades que persiguen la efectiva ejecución de este derecho[902]. Así, en su articulado

[897] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 33; TAJADURA TEJADA, “La Protección...”, cit., 2004, pp. 223-225; CURREA-LUGO, *La Salud*..., cit., 2005, p. 50 y p. 113.
[898] VAQUERO PUERTA, *Salud Pública*...., cit., 1988, p. 26; NAVARRO LÓPEZ, “Concepto Actual...”, cit., 1998, pp. 52-53.
[899] PEMAN GAVIN, *Derecho a la salud*..., cit., 1989, p. 88-89.
[900] ÁLVAREZ-CIENFUEGOS SUÁREZ, “La Naturaleza...”, cit., 1999, p. 161.
[901] Exposición de Motivos LGS.
[902] Artículo 1 LGS: “*1. la presente Ley tiene por objeto la regulación general de todas las acciones que permitan hacer efectivo el derecho a la protección de la salud reconocido en el artículo 43 de la y concordantes de la Constitución”*.

enumera con precisión los elementos que componen la protección de la salud[903]. Se podrían resumir en los siguientes: promoción de la salud; promover el interés individual, familiar y social por la salud mediante la adecuada educación sanitaria de la población; garantizar cuantas acciones sanitarias sean necesarias para la prevención de las enfermedades y no sólo la curación de las mismas; garantizar la asistencia sanitaria en todos los casos de pérdida de la salud y promover las acciones necesarias para la rehabilitación funcional y reinserción social del paciente[904].

Como se aprecia, se recogen de manera amplia todas las acciones que puedan afectar a la salud de las personas. Desde las asistenciales hasta las preventivas, pasando por la educación y la investigación. Cabe subrayar las referencias que se hacen a las materias alimentaria, medioambiental o de seguridad laboral, que denotan la preocupación del legislador de abarcar todos los ámbitos que puedan relacionarse con la salud. La propia Ley incide en otros preceptos

[903] A pesar de su amplitud se reproduce el contenido del artículo 18 LGS, por ser ilustrativo de lo que se quiere decir: *"Las Administraciones públicas, a través de sus servicios de salud y de los órganos competentes en cada caso, desarrollarán las siguientes actuaciones:*
1. Adopción sistemática de acciones para la educación sanitaria como elemento primordial para la mejora de la salud individual y comunitaria, comprendiendo la educación diferenciada sobre los riesgos, características y necesidades de mujeres y hombres, y la formación contra la discriminación de las mujeres.
2. La atención primaria integral de la salud, incluyendo, además de las acciones curativas y rehabilitadoras, las que tiendan a la promoción de la salud y a la prevención de la enfermedad del individuo y de la Comunidad.
3. La asistencia sanitaria especializada, que incluye la asistencia domiciliaria, la hospitalización y la rehabilitación.
4. La prestación de los productos terapéuticos precisos, atendiendo a las necesidades diferenciadas de mujeres y hombres.
5. Los programas de atención a grupos de población de mayor riesgo y programas específicos de protección frente a factores de riesgo, así como los programas de prevención de las deficiencias, tanto congénitas como adquiridas.
6. La promoción y la mejora de los sistemas de saneamiento, abastecimiento de aguas, eliminación y tratamiento de residuos líquidos y sólidos; la promoción y mejora de los sistemas de saneamiento y control del aire, con especial atención a la contaminación atmosférica; la vigilancia sanitaria y adecuación a la salud del medio ambiente en todos los ámbitos de la vida, incluyendo la vivienda.
7. Los programas de orientación en el campo de la planificación familiar y la prestación de los servicios correspondientes.
8. La promoción y mejora de la salud mental.
9. La protección, promoción y mejora de la salud laboral, con especial atención al acoso sexual y al acoso por razón de sexo.
10. El control sanitario y la prevención de los riesgos para la salud derivados de los productos alimentarios, incluyendo la mejora de sus cualidades nutritivas.
11. El control sanitario de los productos farmacéuticos, otros productos y elementos de utilización terapéutica, diagnóstica y auxiliar y de aquellos otros que, afectando al organismo humano, puedan suponer un riesgo para la salud de las personas.
12. Promoción y mejora de las actividades de veterinaria de salud pública, sobre todo en las áreas de la higiene alimentaria, en mataderos e industrias de su competencia, y en la armonización funcional que exige la prevención y lucha contra la zoonosis.
13. La difusión de la información epidemiológica general y específica para fomentar el conocimiento detallado de los problemas de salud.
14. La mejora y adecuación de las necesidades de formación del personal al servicio de la organización sanitaria, incluyendo actuaciones formativas dirigidas a garantizar su capacidad para detectar, prevenir y tratar la violencia de género.
15. El fomento de la investigación científica en el campo específico de los problemas de salud, atendiendo a las diferencias entre mujeres y hombres.
16. El control y mejora de la calidad de la asistencia sanitaria en todos sus niveles.
17. El tratamiento de los datos contenidos en registros, encuestas, estadísticas u otros sistemas de información médica para permitir el análisis de género, incluyendo, siempre que sea posible, su desagregación por sexo".
[904] Artículo 6 LGS.

sobre la especial importancia de tomar en consideración y regular estos ámbitos. Así, se reconoce la necesidad de que las autoridades sanitarias participen en la elaboración de la legislación medioambiental en materias como el aire, aguas, residuos orgánicos, suelo, sustancias tóxicas, etc[905], o se somete a autorización y registro a empresas o productos por razones sanitarias, se prohíbe o limita el uso y tráfico de bienes que puedan suponer un riesgo para la salud o se interviene en las actividades que tienen una repercusión excepcional y negativa en la salud de los ciudadanos con el fin de eliminarlas[906]. De la misma forma se hace también concreta referencia a la necesidad de articular todos los mecanismos necesarios para garantizar la salud en el ámbito laboral[907].

Cabe subrayar la incidencia que hace esta norma sobre los aspectos dirigidos a la prevención de los riesgos para la salud. La consideración expresa de esta actividad preventiva como una pieza fundamental en la protección de la salud no deja lugar a dudas[908]. La docencia en materia sanitaria cuenta también con una referencia expresa que resalta su importancia como actividad dirigida, aunque quizás de manera no inmediata, a la protección de la salud[909]. La investigación y la realización de los estudios epidemiológicos, que son reconocidos por la LGS, cuentan con una regulación propia que más adelante será citada.

También desde una perspectiva general, la Ley de Cohesión y Calidad del Sistema Nacional de Salud entra a regular la actividad sanitaria. En este caso la finalidad es establecer acciones de coordinación entre las diferentes administraciones con el fin de garantizar a todos los ciudadanos su derecho a la protección de la salud[910]. Esta norma entra a determinar, al igual que lo hizo la LGS, las actividades que componen el derecho a la protección de la salud. Reconoce que se engloban prestaciones de salud pública, de atención primaria, de atención especializada, de atención sociosanitaria, de urgencia, farmacéutica, ortoprotésica, de productos dietéticos y de transporte sanitario, para después concretar las actividades que engloba cada una de las prestaciones[911]. Detalla esta norma qué actividades integran cada una de las fases que componen la protección de la salud. Por un lado la asistencia sanitaria directa sobre cada paciente y por otro la actividad preventiva[912], donde, una vez más, se hace expresa mención a

[905] Artículo 19 LGS.
[906] Artículo 25 LGS.
[907] Artículo 21 LGS.
[908] Artículo 8 LGS.
[909] Artículo 104 LGS.
[910] Exposición de Motivos, Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.
[911] Artículo 7.1 Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.
[912] Se estima necesario reproducir el contenido de diferentes preceptos de la Ley debido a su especial interés: Artículo 12 Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: *"Prestación de atención primaria.*
1. La atención primaria es el nivel básico e inicial de atención, que garantiza la globalidad y continuidad de la atención a lo largo de toda la vida del paciente, actuando como gestor y coordinador de casos y regulador de flujos. Comprenderá actividades de promoción de la salud, educación sanitaria, prevención de la enfermedad, asistencia sanitaria, mantenimiento y recuperación de la salud, así como la rehabilitación física y el trabajo social.
2. La atención primaria comprenderá:
a. La asistencia sanitaria a demanda, programada y urgente tanto en la consulta como en el domicilio del enfermo.
b. La indicación o prescripción y la realización, en su caso, de procedimientos diagnósticos y terapéuticos.
c. Las actividades en materia de prevención, promoción de la salud, atención familiar y atención comunitaria.
d. Las actividades de información y vigilancia en la protección de la salud.
e. La rehabilitación básica.

f. Las atenciones y servicios específicos relativos a las mujeres, que específicamente incluirán la detección y tratamiento de las situaciones de violencia de género; la infancia; la adolescencia; los adultos; la tercera edad; los grupos de riesgo y los enfermos crónicos.
g. La atención paliativa a enfermos terminales.
h. La atención a la salud mental, en coordinación con los servicios de atención especializada.
i. La atención a la salud bucodental."
Artículo 13. *"Prestación de atención especializada.*
1. La atención especializada comprende actividades asistenciales, diagnósticas, terapéuticas y de rehabilitación y cuidados, así como aquéllas de promoción de la salud, educación sanitaria y prevención de la enfermedad, cuya naturaleza aconseja que se realicen en este nivel. La atención especializada garantizará la continuidad de la atención integral al paciente, una vez superadas las posibilidades de la atención primaria y hasta que aquel pueda reintegrarse en dicho nivel.
2. La atención sanitaria especializada comprenderá:
a. La asistencia especializada en consultas.
b. La asistencia especializada en hospital de día, médico y quirúrgico.
c. La hospitalización en régimen de internamiento.
d. El apoyo a la atención primaria en el alta hospitalaria precoz y, en su caso, la hospitalización a domicilio.
e. La indicación o prescripción, y la realización, en su caso, de procedimientos diagnósticos y terapéuticos.
f. La atención paliativa a enfermos terminales.
g. La atención a la salud mental.
h. La rehabilitación en pacientes con déficit funcional recuperable.
3. La atención especializada se prestará, siempre que las condiciones del paciente lo permitan, en consultas externas y en hospital de día".
Artículo 14. *"Prestación de atención sociosanitaria.*
1. La atención sociosanitaria comprende el conjunto de cuidados destinados a aquellos enfermos, generalmente crónicos, que por sus especiales características pueden beneficiarse de la actuación simultánea y sinérgica de los servicios sanitarios y sociales para aumentar su autonomía, paliar sus limitaciones o sufrimientos y facilitar su reinserción social.
2. En el ámbito sanitario, la atención sociosanitaria se llevará a cabo en los niveles de atención que cada comunidad autónoma determine y en cualquier caso comprenderá:
a. Los cuidados sanitarios de larga duración.
b. La atención sanitaria a la convalecencia.
c. La rehabilitación en pacientes con déficit funcional recuperable.
3. La continuidad del servicio será garantizada por los servicios sanitarios y sociales a través de la adecuada coordinación entre las Administraciones públicas correspondientes."
Artículo 15. "*Prestación de atención de urgencia.*
La atención de urgencia se presta al paciente en los casos en que su situación clínica obliga a una atención sanitaria inmediata. Se dispensará tanto en centros sanitarios como fuera de ellos, incluyendo el domicilio del paciente, durante las 24 horas del día, mediante la atención médica y de enfermería".
Artículo 16. *"Prestación farmacéutica.*
La prestación farmacéutica comprende los medicamentos y productos sanitarios y el conjunto de actuaciones encaminadas a que los pacientes los reciban de forma adecuada a sus necesidades clínicas, en las dosis precisas según sus requerimientos individuales, durante el período de tiempo adecuado y al menor coste posible para ellos y la comunidad.
Esta prestación se regirá por lo dispuesto en la Ley 25/1990, de 20 de diciembre, del Medicamento, y por la normativa en materia de productos sanitarios y demás disposiciones aplicables".
Artículo 17. *"Prestación ortoprotésica.*
La prestación ortoprotésica consiste en la utilización de productos sanitarios, implantables o no, cuya finalidad es sustituir total o parcialmente una estructura corporal, o bien de modificar, corregir o facilitar su función. Comprenderá los elementos precisos para mejorar la calidad de vida y autonomía del paciente.
Esta prestación se facilitará por los servicios de salud o dará lugar a ayudas económicas, en los casos y de acuerdo con las normas que reglamentariamente se establezcan por parte de las Administraciones sanitarias competentes".
Artículo 18. *"Prestación de productos dietéticos.*
La prestación de productos dietéticos comprende la dispensación de los tratamientos dietoterápicos a las personas que padezcan determinados trastornos metabólicos congénitos, la nutrición enteral domiciliaria para pacientes a los que no es posible cubrir sus necesidades nutricionales, a causa de su situación clínica, con alimentos de uso ordinario.
Esta prestación se facilitará por los servicios de salud o dará lugar a ayudas económicas, en los casos y de acuerdo con las normas que reglamentariamente se establezcan por parte de las Administraciones sanitarias competentes".

aspectos vinculados al medioambiente, salud laboral o seguridad alimentaria. También en esta norma se resalta la importancia de actividades como la docencia[913] o la investigación[914]. Por último, la protección de la salud exige también que se lleven a cabo actuaciones de gestión estrictamente administrativa, como puede ser el caso de la inspección. El funcionamiento de cualquier sistema sanitario depende de una buena gestión, económica, personal, de información, etc.

Otra norma fundamental dirigida a la regulación de la actividad sanitaria es la LBAP. Cuando se refiere a los usos que se pueden dar a la historia clínica recoge también un concepto amplio de lo que es la actividad sanitaria[915]. Reconoce como actividad principal la asistencial, pero se refiere también a los fines epidemiológicos, de salud pública, de investigación, de docencia, e incluso judiciales, a los que más adelante se hará mención. Se hace referencia expresa también a la actividad administrativa o de gestión, poniendo énfasis en las funciones de inspección, planificación, acreditación o evaluación. La interpretación que realiza esta norma sobre el alcance de la protección de la salud es de especial interés aquí. Como se irá viendo, esta Ley servirá para deducir importantes claves sobre cómo se pueden manipular los datos de carácter sanitario.

Las normas que se acaban de citar reflejan, aunque sólo sea de manera somera, el ámbito que abarca el derecho a la protección de la salud. Se trata de acciones de diferente tipo, asistenciales o de prevención. Estos ámbitos son concretados después por una extensa normativa sanitaria que desarrolla esta regulación general. No se cree necesario exponer aquí todas las normas que entran a regular la materia sanitaria, basta con apuntar algunas a modo de ejemplo, que pueden tener un interés especial por su afección al derecho fundamental a la autodeterminación informativa.

Artículo 19." *Prestación de transporte sanitario.*
El transporte sanitario, que necesariamente deberá ser accesible a las personas con discapacidad, consiste en el desplazamiento de enfermos por causas exclusivamente clínicas, cuya situación les impida desplazarse en los medios ordinarios de transporte. Esta prestación se facilitará de acuerdo con las normas que reglamentariamente se establezcan por las Administraciones sanitarias competentes."
Artículo 11, Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: *"Prestaciones de salud pública.*
1. La prestación de salud pública es el conjunto de iniciativas organizadas por las Administraciones públicas para preservar, proteger y promover la salud de la población. Es una combinación de ciencias, habilidades y actitudes dirigidas al mantenimiento y mejora de la salud de todas las personas a través de acciones colectivas o sociales.
2. Las prestaciones en este ámbito comprenderán las siguientes actuaciones:
a. La información y vigilancia epidemiológica.
b. La protección de la salud.
c. La promoción de la salud.
d. La prevención de las enfermedades y de las deficiencias.
e. La vigilancia y control de los posibles riesgos para la salud derivados de la importación, exportación o tránsito de mercancías y del tráfico internacional de viajeros, por parte de la Administración sanitaria competente.
f. La promoción y protección de la sanidad ambiental.
g. La promoción y protección de la salud laboral, con especial consideración a los riesgos y necesidades específicos de las trabajadoras.
h. La promoción de la seguridad alimentaria.
3. Las prestaciones de salud pública se ejercerán con un carácter de integralidad, a partir de las estructuras de salud pública de las Administraciones y de la infraestructura de atención primaria del Sistema Nacional de Salud."
[913] Capítulo III, Sección I, Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.
[914] Capítulo IV, Sección I, Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud.
[915] Artículo 16 LBAP.

La Ley orgánica de Medidas Especiales en Materia de Salud[916] recoge supuestos en que las autoridades públicas, en determinadas situaciones de emergencia, pueden adoptar medidas de naturaleza excepcional que afectan directamente a derechos fundamentales, como la autodeterminación informativa o incluso la libertad de los ciudadanos, con el fin de salvaguardar la salud pública[917]. En este caso la norma adopta la forma de Ley orgánica debido a que el legislador entra a desarrollar diferentes derechos fundamentales que se ven afectados por la adopción de estas medidas excepcionales.

La actual Ley del Medicamento[918] concreta el derecho a la protección de la salud en un ámbito tan específico como es el de la regulación de los medicamentos[919]. En lo que afecta a la manipulación de los datos de carácter personal, la Ley viene a trazar las líneas maestras de lo que se entiende por farmacovigilancia[920] y ensayos clínicos[921], dos actividades dirigidas a la salvaguarda, fundamentalmente, de la salud pública y que en determinados casos pueden requerir de la manipulación de datos de carácter personal. Esta norma viene a fijar también los aspectos más importantes que hay que tener en cuenta en la distribución de los medicamentos a los pacientes, a través de recetas médicas incluso electrónicas, ejercicio que necesariamente requiere del empleo de datos sanitarios[922].

La Ley sobre Técnicas de Reproducción Humana Asistida[923] determina también otro ámbito que puede afectar a la salud de las personas y en la que el tratamiento de datos de carácter personal, sobre todo del donante de gametos y preembriones, resulta un instrumento

[916] LO 3/1986, 14 de abril, Medidas Especiales en Materia de Salud.
[917] Artículo 1 LO 3/1986, 14 de abril, Medidas Especiales en Materia de Salud: "*Al objeto de proteger la salud pública y prevenir su perdida o deterioro, las autoridades sanitarias de las distintas Administraciones públicas podrán, dentro del ámbito de sus competencias, adoptar las medidas previstas en la presente Ley cuando así lo exijan razones sanitarias de urgencia o necesidad"*.
Artículo 2. "*Las autoridades sanitarias competentes podrán adoptar medidas de reconocimiento, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad"*.
Artículo 3. *"Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible"*.
[918] Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios.
[919] Artículo 1.1 Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios: "*La Ley regula, en el ámbito de las competencias que corresponden al Estado, los medicamentos de uso humano y productos sanitarios, su investigación clínica, su evaluación, autorización, registro, fabricación, elaboración, control de calidad, almacenamiento, distribución, circulación, trazabilidad, comercialización, información y publicidad, importación y exportación, prescripción y dispensación, seguimiento de la relación beneficio-riesgo, así como la ordenación de su uso racional y el procedimiento para, en su caso, la financiación con fondos públicos. La regulación también se extiende a las sustancias, excipientes y materiales utilizados para su fabricación, preparación o envasado*".
[920] Artículo 53 y siguientes de la Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios.
[921] Artículo 58 y siguientes de la Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios.
[922] Artículo 77 de la Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios.
[923] Ley 14/2006, 26 de mayo, sobre Técnicas de Reproducción Humana Asistida.

fundamental, tanto para llevar a cabo las operaciones de reproducción asistida admitidas en la norma como para la investigación en este y otros campos[924].

La reciente Ley de Investigación Biomédica[925] desarrolla la Constitución en el punto que obliga a los poderes públicos, a promover la ciencia y la investigación científica y técnica a favor del interés común[926]. Regula una realidad que está adquiriendo especial importancia en el sector de la sanidad. Se trata del estudio de muestras biológicas de los individuos, con especial referencia por su relevancia a los análisis genéticos, con el fin de descubrir nuevos métodos de prevención y tratamiento de enfermedades. Esta actividad adquiere una relevancia especial pues se refiere, en muchas ocasiones, a investigaciones de carácter internacional. Evidentemente, del análisis de estas muestras derivará información concerniente a individuos determinados, información que habrá de ser protegida y sobre la cual el titular ha de poder ejercer su derecho a la autodeterminación informativa.

De todas las normas que se acaban de citar se deduce el ámbito de realidad al que se refiere la protección de la salud. Cuando se afirma que los datos de carácter personal podrán ser manipulados con esta finalidad, hay que entender que se engloban todas estas acciones. Sin embargo, hay que aclarar, esto no quiere decir que todas estas actividades tengan la misma incidencia en la salud de las personas y que, por lo tanto, una hipotética limitación al derecho fundamental a la autodeterminación informativa actúa de igual manera cuando se trata de asistir a un individuo en una situación de urgencia médica o cuando la actividad a desarrollar sea la docencia. Como se verá, la ponderación entre los bienes jurídicos en juego deberá realizarse caso por caso, atendiendo a la actividad concreta de la que se trate.

II.2.3.C. La necesidad de que la finalidad sea determinada y específica cuando los datos son tratados en el ámbito sanitario.

Cuando la LOPD requiere que la finalidad sea determinada y explícita se está exigiendo que se concreten las actividades a las que se destinarán los datos. De esta manera, cuando los datos se emplean en el campo sanitario cabe preguntarse si, a efectos de aplicar la Ley, es suficiente con señalar que serán manipulados con la genérica finalidad de proteger la salud de las personas o si es necesario concretar, en la medida de lo posible, dicho campo de actuación. La necesidad de que la finalidad sea concretada al máximo puede fundamentarse en dos argumentos.

Por un lado, al informar al ciudadano sobre la finalidad a la que se va a destinar el tratamiento de sus datos, no basta con indicarle que los datos serán utilizados con la genérica finalidad de proteger la salud, sino que será precisa una mayor concreción de la finalidad. Esta cuestión será analizada cuando se estudie el derecho al consentimiento informado, no obstante, puede adelantarse el siguiente argumento. El derecho del titular a controlar lo que sucede con los datos que le conciernen exige que sea informado sobre la determinada finalidad a la que se van a destinar. La protección de la salud constituye una finalidad genérica que ha de ser detallada. La

[924] Artículo 14 y siguientes de la Ley 14/2006, de 26 de mayo, sobre Técnicas de Reproducción Humana Asistida.
[925] Ley 14/2007, 3 de julio, de Investigación Biomédica.
[926] Artículo 44.2 CE.

opción opuesta podría dejar desprotegido al usuario ante determinadas situaciones. Por ejemplo, una cosa es que una muestra de sangre de una persona sea empleada para hacer unos análisis cuyos resultados serán utilizados en la asistencia médica directa a dicho individuo, y otra que la muestra y los resultados de dichos análisis sean remitidos a una empresa privada colaboradora con la Administración para llevar a cabo diferentes investigaciones de carácter científico. Ambas actividades podrían englobarse en la genérica finalidad de protección de la salud, sin embargo, es indudable que la reacción del titular de los datos ante una u otra función sería distinta.

Por otro lado, se ha dicho que el derecho a la protección de la salud puede constituir un límite al derecho fundamental a la autodeterminación informativa. No obstante, se verá que no todas las actividades que completan la salvaguarda de la salud entran a colisionar de la misma manera con el derecho fundamental citado. La aplicación del principio de proporcionalidad requerirá de un juicio ponderativo en cada caso. Es por ello necesario que las finalidades a las que se destinan los tratamientos de datos sean determinadas con el máximo rigor.

La concreción de la finalidad no será, en principio, una tarea compleja si se tiene en cuenta que las normas que crean los ficheros con los que cuenta la Administración sanitaria determinan en principio los objetivos a los que se destinarán. Como exige la LOPD, la creación de los ficheros de las Administraciones públicas sólo puede hacerse por Disposición General publicada en el Diario Oficial correspondiente[927]. En estas disposiciones se especifican cuáles son las finalidades concretas que motivan la recogida y tratamiento de los datos y qué órganos tendrán acceso a dicha información. Los Acuerdos del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los Ficheros Automatizados de Datos de Carácter Personal gestionados por Osakidetza-Servicio Vasco de Salud, pueden constituir un ejemplo de lo que se ha explicado[928]. Precisamente, en estas normas se recogen ficheros con los que cuenta el sistema sanitario vasco determinándose su finalidad. Ficheros con muy diferente contenido se utilizan en este ámbito. Algunos con finalidad estrictamente administrativa o de gestión económica que no contienen en general datos de contenido puramente médico o sanitario y otros con contenido estrictamente médico, como puede ser el registro de casos de sida o el registro de tumores o el de Historias Clínicas. Cada fichero se crea con una finalidad determinada que justificará el tratamiento de los datos de carácter personal en un régimen concreto. Por ejemplo, el Registro de casos de Sida tiene por finalidad contabilizar el número de casos de SIDA en la CAPV, la vigilancia epidemiológica, el tratamiento estadístico de la información obtenida, la realización de estudios epidemiológicos, la investigación y planificación sanitaria y la entrega de cartilla sanitaria específica para enfermos de SIDA[929]. Como se ve, si

[927] Artículo 20.1 LOPD.

[928] Acuerdo de 17 de marzo de 2008, del Consejo de Administración del Ente Público Osakidetza, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud, BOPV nº 192, del 8 de octubre de 2008 que reforma en algunos puntos el anterior Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los Ficheros Automatizados de Datos de Carácter Personal gestionados por Osakidetza-Servicio Vasco de Salud.

[929] Anexo II, 4.1, Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los Ficheros Automatizados de Datos de Carácter Personal gestionados por Osakidetza-Servicio Vasco de Salud.

bien es cierto que en estas normas también pueden encontrarse cláusulas genéricas[930], las finalidades a las que se destinarán los datos aparecen bien definidas, por lo que el requisito de que los fines sean concretos, con vistas a la salvaguarda del derecho a la autodeterminación informativa, será de fácil realización.

III. EL PRINCIPIO DE PERTINENCIA EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL POR LA ADMINISTRACIÓN SANITARIA.

Ya se ha subrayado al iniciar este apartado que entre los principios que determinan la calidad de los datos el de finalidad se erige en el más relevante. Sin duda alguna, este principio constituye una de las columnas vertebrales, quizás la más importante, de la regulación del derecho a la autodeterminación informativa. No obstante, junto al de finalidad la LOPD reconoce dentro de los denominados principios de calidad los de pertinencia y de veracidad. Al primero de ellos se va a hacer referencia a continuación.

III.1. La pertinencia como sinónimo del principio de proporcionalidad en la LOPD.

La LOPD, siguiendo lo que señalaba la anterior normativa reguladora de la protección de datos, dispone que sólo pueden recogerse y tratarse datos de carácter personal para el cumplimiento de una finalidad determinada, siempre y cuando esos datos sean *"adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se hayan obtenido*"[931]. El reglamento que desarrolla la Ley recoge una regulación prácticamente idéntica, si bien introduce algún cambio que más adelante se comentará debido a su importancia[932]. Lo mismo hace la Directiva europea, que reconoce la necesidad de que todo dato que vaya a ser manipulado sea adecuado, pertinente y no excesivo en relación a los objetivos perseguidos con el tratamiento[933]. El contenido del Convenio del Consejo de Europa es también muy similar en este aspecto[934].

De una primera lectura de estas normas se podría deducir que el principio de pertinencia recoge simplemente una regla que todo tratamiento de datos ha de seguir: cuando se quieran manipular datos de carácter personal para conseguir un fin, sólo podrán tratarse los datos estrictamente pertinentes para la consecución de dicho objetivo. Sin embargo, de un análisis más profundo de la letra de la Ley se concluye que este principio merece un estudio más riguroso, que requiere de su puesta en común con conocidos principios generales de la teoría general de los derechos humanos.

---

[930] Acuerdo Tercero, Acuerdo de 17 de marzo de 2008, del Consejo de Administración del Ente Público Osakidetza, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud: "*1. Los ficheros objeto del presente Acuerdo, además de servir a los fines que para cada uno se indican en el correspondiente anexo, tendrán como objetivo la realización de estudios epidemiológicos y la investigación sanitaria. Asimismo, tendrán como finalidad su utilización estadística*".

[931] Artículo 4.1 LOPD.

[932] Artículo 8.4 RDLOPD.

[933] Considerando 28 Directiva 95/46/CE: "*Considerando que todo tratamiento de datos personales debe (...) referirse, en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos (...)*"; Artículo 6.1 Directiva 95/46/CE: "*Los Estados miembros dispondrán que los datos sean (...) c) adecuados pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente*".

[934] Artículo 5 Convenio 108/1981 del Consejo de Europa.

El principio de pertinencia constituye en sí mismo una regla a respetar por toda manipulación de datos. En un primer acercamiento a las definiciones dadas se deduce que lo que exige este principio es, simplemente, que para cumplir una finalidad determinada sólo se deben manipular los datos estrictamente pertinentes. Esta regla tiene pleno sentido desde la perspectiva del respeto al derecho fundamental a la autodeterminación informativa. Si en atención al principio de finalidad los datos de carácter personal sólo pueden recogerse y tratarse para llevar a cabo un fin determinado, explícito y legítimo, lo lógico y exigible para el respeto a este derecho es que los datos que se recojan y traten con ese fin sean los estrictamente necesarios para llevar a cabo el mismo. Si se manipularan más datos de los indispensables el derecho a la autodeterminación informativa se vería innecesariamente afectado. De esta manera, lo que en última instancia exige esta regla es que en el ejercicio de la manipulación de datos con una finalidad determinada se cause el menor daño posible al citado derecho fundamental[935].

El principio de pertinencia pone en relación los datos que se recogen y la finalidad concreta para la que se recogen, es decir, el medio para conseguir un fin y el fin en sí mismo. La manipulación de la información no es más que un medio para conseguir una finalidad. En el caso que en este trabajo se trata el objetivo será salvaguardar la salud de los ciudadanos. Pues bien, en base al principio que se analiza, tiene que haber una coherencia o relación entre dicho medio y el fin. Esta coherencia se traduce en la necesidad de que con el empleo del medio se cause el menor daño posible para conseguir el fin que se pretende, es decir, que el tratamiento de datos que se vaya a llevar a cabo para cumplir con el objetivo de proteger la salud de las personas afecte en la menor medida posible al derecho fundamental a la autodeterminación informativa.

El tratamiento por un agente que no sea el titular de unos datos de carácter personal supone en todo caso una afección al derecho fundamental a la autodeterminación informativa. Esta afección necesariamente ha de estar justificada. La justificación vendrá de la mano del consentimiento de dicho titular de los datos para tratarlos o de la habilitación de una Ley, que reconoce que la manipulación de los datos de carácter personal es necesaria para la salvaguarda de un bien jurídico de mayor entidad. Pues bien, para que dicha justificación sea válida será necesario que haya una coherencia entre los datos que se tratan y la finalidad que se persigue. El responsable del fichero no podrá recabar ni tratar más datos de los estrictamente necesarios para alcanzar el fin que se propone[936]. La coherencia se traduce en el principio de pertinencia.

En los casos en que la jurisprudencia se ha pronunciado sobre el sentido de este principio ha remarcado la obligación de que los datos que se traten en cada caso sean los estrictamente necesarios y adecuados para el cumplimiento del fin pretendido[937]. La AEPD también ha subrayado la importancia del principio de pertinencia en alguna recomendación. Concretamente, en relación a una cuestión tan compleja como es la contratación de empleados a través de Internet, pone de manifiesto la importancia de que sólo se recaben los datos necesarios relativos

[935] Resolución de la AEPD, R/01235/2007, de 21 de diciembre de 2007, procedimiento PS/00182/2007.
[936] REBOLLO DELGADO, *Derechos Fundamentales*..., cit., 2004, p. 146; APARICIO SALOM, "La calidad…", cit., 2010, p. 233, se refiere a que más allá de que el responsable del fichero cuente con el consentimiento del titular, será necesario, siempre, que haya una relación entre el fin que se persigue con el tratamiento de datos y la información que se manipula.
[937] STC 20 de julio de 1993, FJ 7.

a los candidatos. Reconoce esta institución que las empresas tienden, cuando emplean Internet con el fin de contratar personas, a solicitar y manipular datos que tienen que ver más con la vida personal o la ideología que con su vida profesional[938].

Es evidente que en el precepto que se analiza se recoge un criterio determinado y claro sobre cómo han de manipularse los datos. Sin embargo, esta previsión constituye, como se verá a continuación, la concreción en un aspecto específico de un principio general de especial relevancia en materia de derechos humanos. Se está haciendo referencia al principio de proporcionalidad. De esta manera, más allá de establecer una regla o criterio que toda manipulación de información ha de respetar, el principio de pertinencia reconocido en las normas de protección de datos constituye un llamamiento expreso a la incorporación a este ámbito del principio de proporcionalidad.

La vinculación entre la regla establecida en la LOPD y el principio general de proporcionalidad resulta clara. Este último es un pilar fundamental en la regulación de los derechos humanos y así, siendo para la mayoría de agentes jurídicos el derecho a la autodeterminación informativa un derecho fundamental autónomo, su aplicación no resulta extraña. El principio de proporcionalidad constituye un criterio general a seguir para determinar la validez de los límites que se quieran imponer a los derechos. Concretamente, exige que en la persecución de un fin concreto, cuando un derecho ha de verse afectado negativamente, dicha afección sea la mínima posible[939]. Obliga a que en la consecución de un fin se adopte el medio menos gravoso para los derechos e intereses de las personas afectadas. Es decir, trata de encontrar un equilibrio justo cuando diferentes derechos, intereses o bienes colisionan. Por ejemplo, este principio entraría en juego en la medida en que el derecho a la autodeterminación informativa se ve limitado en diferentes aspectos, cuando se manipulan datos de carácter personal con la finalidad de proteger la salud de las personas. Piénsese en el supuesto en que se exceptúa el derecho a consentir un tratamiento de datos por el hecho de que el objetivo es la protección de la salud de un sujeto. El genérico principio de proporcionalidad exige que esa limitación sea la mínima posible.

Atendiendo al contenido del principio de proporcionalidad resulta obvia la vinculación entre éste y el principio de pertinencia. Los criterios a seguir que derivan de ambos convergen irremediablemente. Según la letra de la LOPD sólo se deberán tratar los datos estrictamente necesarios para conseguir la finalidad que se pretende. Si se manipula más información de la debida se estará afectando injustificadamente al derecho citado. Esta regla no es otra cosa que la concreción del principio de proporcionalidad, que exige que los límites externos que se traten de imponer a los derechos afecten en la menor medida posible a dichos derechos. Si las excepciones a las facultades que componen la autodeterminación informativa van más allá de lo estrictamente debido estarán afectando innecesariamente al derecho. El significado del criterio a respetar es siempre el mismo: toda medida que afecte negativamente al derecho fundamental a la autodeterminación informativa ha de causar el menor daño posible. En este sentido la

[938] Recomendación de la AEPD, "Selección de Personal a través de Internet", de 17 de noviembre de 2005.
[939] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p. 304.

vulneración del principio concreto de pertinencia no es otra cosa que la vulneración del principio genérico de proporcionalidad.

En definitiva, es indudable que la incorporación en la LOPD del principio de pertinencia, como se ha calificado por la doctrina, constituye el reconocimiento en el ámbito de la protección de datos del principio de proporcionalidad[940]. Muestra de ello es que en ocasiones la jurisprudencia emplea el término proporcionalidad para hacer referencia a la exigencia planteada por la Ley, de que exista un equilibrio entre las finalidades que se persiguen y los datos que se manipulan[941]. Así lo hace también la AEPD en alguna de sus resoluciones[942]. En este sentido cabe destacar cómo en algún caso la APDCM ha llevado a cabo, en atención al principio de pertinencia, un juicio de proporcionalidad completo teniendo en cuenta los criterios de adecuación, necesidad y proporcionalidad en sentido estricto, para llegar a la conclusión de que establecer un sistema de gestión de control de horario del personal al servicio de la Administración de Justicia dependiente de la Comunidad de Madrid, basado en el uso de las huellas de los trabajadores, constituye una medida pertinente o proporcional en relación a la finalidad[943]. En la misma línea, ya en el debate parlamentario sobre la aprobación de la LOPD se planteó la posibilidad de incorporar expresamente el concepto de proporcionalidad en el artículo concerniente a la pertinencia[944].

En cualquier caso, bajo el nombre de proporcionalidad o pertinencia, se va a analizar a continuación la necesidad de que exista una relación coherente entre un medio, que no es otro que el tratamiento de los datos de carácter personal, y un fin que se pretende lograr con el empleo de dicho medio, que es la salvaguarda de la salud de los ciudadanos. Atendiendo a lo dicho hasta ahora, el análisis del principio de pertinencia recogido en las normas de protección de datos ha de llevar a estudiar algunos aspectos básicos del genérico principio de proporcionalidad[945]. No se va a hacer un estudio completo sobre el mismo entrando a analizar en profundidad el concepto, origen, naturaleza jurídica y demás aspectos que configuran esta institución, sino que se realizará una breve referencia a los elementos que componen el denominado juicio de proporcionalidad, que ayudará a indicar si una manipulación de datos concreta es pertinente en relación a la finalidad que persigue.

III.2. Proporcionalidad. Consideraciones generales.

III.2.1. Su inclusión en el ordenamiento jurídico español.

Para comprender correctamente el contenido de la regla prevista en la normativa de protección de datos es aconsejable analizar, aunque sea de manera somera, una serie de aspectos genéricos sobre el principio de proporcionalidad. Esta labor es procedente en la medida en que a lo largo del trabajo se hará referencia en numerosas ocasiones al citado principio

[940] SANZ CALVO, "Calidad de los Datos"…, cit., 2008, p. 142; AGÚNDEZ LERÍA, "Principios relativos…", cit., 2008, p. 143.
[941] SSAN, 25 de marzo de 2009, FJ 3 y 11 de marzo de 2009, FJ 2.
[942] Resolución de la AEPD, R/00589/2004, de 21 de octubre de 2004, procedimiento AAPP/00013/2004.
[943] Resolución de Archivo de Actuaciones de la APDCM, E/166/2006, de 13 de junio de 2007.
[944] BOCG nº 135-7, Serie A, de 4 de noviembre de 1998, enmienda nº 74 de Coalición Canaria. Justificaba la inclusión del concepto "proporcionales" por su mayor concreción y tradición jurídica.
[945] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...*, cit., 2001, p. 196.

entendido como principio general, ya que son varios los casos en que se analizará la colisión del derecho a la autodeterminación informativa con otros derechos.

Se ha dicho que el principio de proporcionalidad constituye un criterio empleado para dirimir, la mayoría de las veces, los conflictos que pueden generarse cuando diferentes derechos, intereses o bienes jurídicos colisionan entre sí. Su aplicación lleva a que cuando se dan estas situaciones de confrontación, los bienes, derechos e intereses se vean afectados negativamente en la menor medida posible. Es decir, el juicio de proporcionalidad aspira siempre a encontrar el equilibrio más justo entre los intereses en juego.

La inclusión del principio de proporcionalidad en el ordenamiento español es un hecho incuestionable. Este principio, al contrario de lo que ocurre con otros muchos principios generales del derecho, constituye un criterio que no ha sido recogido expresamente por la CE. Ha sido la jurisprudencia la que ha ido determinando su contenido y su modo de aplicación hasta integrarlo en el ordenamiento[946]. Hoy día está comúnmente aceptado que el TC ha hecho suyo el denominado test alemán de proporcionalidad[947]. Según este criterio todo límite a un derecho fundamental ha de respetar los tres subprincipios que componen el citado juicio de proporcionalidad: el subprincipio de adecuación, el de necesidad y el de proporcionalidad en sentido estricto[948].

El sistema de control de los límites a los derechos fundamentales que supone el principio de proporcionalidad, tal como hoy se conoce[949], se crea en Alemania[950] y recala en el ordenamiento español principalmente a través de su aplicación por el TEDH y por el TJUE[951]. Cierto es que en la jurisprudencia de estos tribunales su aplicación no ha sido regular ni ha seguido un esquema o sistema claramente marcado o definido. Sin embargo, el empleo constante del mismo en la toma de sus decisiones ha hecho que su utilización se extienda a ordenamientos como el español que no preveían expresamente su aplicación.

En el caso del TJUE el uso del principio de proporcionalidad como parámetro de control de todo límite a los derechos fundamentales es incuestionable[952]. Su empleo, sin embargo, no ha sido especialmente uniforme[953]. En unos casos parece identificarse con el subprincipio de necesidad[954], en otros con el de idoneidad[955], y en algunos supuestos también se lleva a cabo

[946] GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, p. 29.
[947] SSTC, 10 de julio del 2000, FFJJ 6 y 7y 16 de enero de 2006, FJ 6. BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 334; DE LA MATA BARRANCO, *El Principio de Proporcionalidad…,* cit., 2007, p. 40.
[948] MUÑOZ ARNAU, *Los Límites...*, cit., 1998, p. 153.
[949] LOPERA MESA, *Principio de Proporcionalidad...*, cit., 2006, pp. 30-43: La génesis del citado principio puede remontarse incluso hasta ciertas prácticas de la Grecia antigua.
[950] AGUADO CORREA, *El Principio...*, cit., 1999, p. 63.
[951] BARNES, "Introducción al Principio…", cit., 1994, p. 495; DÍEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 114.
[952] BARNES, "Introducción al Principio…", cit., 1994, p. 519; SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p. 610.
[953] BARNES, "Introducción al Principio…", cit., 1994, p. 521.
[954] STJUE 5 junio 2007, Klasd Rosengren y otros v. Riksaklagarem, asunto C-170/04, FJ 50: "principio de proporcionalidad, es decir, que es necesaria para alcanzar el objetivo invocado, y que dicho objetivo no puede alcanzarse mediante prohibiciones o limitaciones de menor amplitud o que afecten en menor medida al comercio intracomunitario".

exclusivamente el test de proporcionalidad en sentido estricto realizando una ponderación de los bienes jurídicos en juego[956]. En otras sentencias el TJUE parece llevar a cabo un test más completo combinando diferentes requisitos de los citados, especialmente el de adecuación y el de necesidad[957]. En resumen, se puede decir que el TJUE es conocedor de los diferentes elementos que completan el citado test alemán de proporcionalidad, si bien, dependiendo de cada caso concreto, aplica un criterio u otro.

En lo que corresponde al TEDH, según ha explicado la doctrina, el Tribunal viene utilizando el principio de proporcionalidad desde hace tiempo[958], precisamente fundamentándose en el artículo 8 que se refiere a la salvaguarda de la vida privada[959].

El citado artículo lleva necesariamente a realizar un juicio de proporcionalidad[960]. La consideración de que toda limitación a la vida privada tiene que ser "*en una sociedad democrática*" "*necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral o la protección de los derechos y las libertades de los demás*", es un llamamiento a la aplicación del principio de proporcionalidad, como el propio Tribunal europeo ha reconocido[961]. Ya desde un inicio expuso que en la consecución de un fin tan importante como es la lucha contra el terrorismo no todo vale y que, a la hora de tomar las medidas oportunas para conseguir el indicado fin, han de adoptarse todas las garantías posibles que hagan precisamente que estas medidas sean proporcionales en relación al objetivo perseguido[962].

Sin embargo, más que llevar a cabo un análisis sistemático de los elementos que componen el test de proporcionalidad, normalmente realiza un juicio genérico de proporcionalidad para determinar si la medida que se aplica es coherente con la finalidad que se pretende[963]. No parece llevarse a cabo en el ámbito del TEDH un estudio tan riguroso como parece hacerlo por ejemplo el TC, que sigue el esquema alemán que más adelante se verá y que entiende que una medida será proporcional con respecto a un fin cuando sea adecuado, necesario y proporcional en sentido estricto, para alcanzar el fin[964]. En la mayoría de los análisis que el TEDH realiza la principal cuestión que se atiende es el de la proporcionalidad en sentido estricto. Así, a la hora de determinar si un medio es proporcional con respecto al fin que se persigue, la cuestión fundamental a dilucidar es la colisión entre los bienes jurídicos en juego. Se trata de analizar el

[955] STJUE 4 junio 2002, Comisión de las Comunidades Europeas v. Bélgica, asunto C-367/98, FJ 33: "En su opinión, también se cumple el criterio de proporcionalidad. En efecto, el examen de las operaciones que modifican la estructura del accionariado constituye un medio apropiado para alcanzar el objetivo perseguido".
[956] STJUE 6 diciembre 2001, Consejo de la UE v. Heidi Hautala, asunto C-353/99, FJ 85 y siguientes.
[957] SSTJUE, 18 septiembre 1986, C-116/82, FJ 21; 15 mayo 1986, C-222/84, FJ 38; 10 marzo 1987, asuntos acumulados 279, 280, 285 y 286/84; 11 julio 1989, asunto C-265/87, FFJJ 20 y 21; 27 junio 1990, Firma Otto Lingenfelser v. República Federal de Alemania, asunto C-118/89, FJ 12.
[958] BRAGE CAMAZANO,"Aproximación a una Teoría…", cit., 2005 p. 132.
[959] LOPERA MESA, *Principio de Proporcionalidad*..., cit., 2006, p. 39.
[960] ARZOZ SANTIESTEBAN, "Comentario al...", cit., 2009, p. 298.
[961] STEDH 22 marzo 2007, Maslov c. Austria, FJ 33.
[962] SSTEDH, 6 septiembre 1978, Klass y otros c. Alemania, FJ 50 y 26 marzo 1987, Leander c. Suecia, FJ 58 y siguientes.
[963] AGUADO CORREA, *El Principio de Proporcionalidad…,* cit., 1999, p. 61.
[964] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p.703.

peso de los intereses en conflicto, de buscar el equilibrio entre el bien jurídico que representa el fin frente al bien jurídico que se ve afectado con el empleo del medio[965]. En todo caso, es patente el empleo por parte de este Tribunal del principio de proporcionalidad a la hora de determinar la coherencia existente entre un medio limitador de un derecho fundamental y un fin[966].

En algún caso el TEDH ha concluido que para justificar una limitación de un derecho fundamental, para la consecución de un fin determinado, dicha limitación deberá constituir una "necesidad social imperiosa"[967]. Ciertamente, de esta expresión se deduce todo lo necesario para comprender correctamente el principio de proporcionalidad.

La importancia de las decisiones del TEDH en el ámbito interno es conocida. Su influencia real en el derecho interno es limitada, sin embargo, merece la pena llevar a cabo un apunte sobre esta cuestión para comprender el alcance de sus sentencias sobre materias que conciernen, por ejemplo, a la protección de datos. La doctrina, siguiendo al TC, ha asumido que las sentencias de esta instancia no tienen carácter ejecutivo sino meramente declarativo[968]. Una sentencia de este Tribunal no anula una sentencia del TC o del Tribunal Supremo, ni una norma emitida en el ámbito interno[969]. Sin embargo, esto no quiere decir que los Estados firmantes del Convenio no han de cumplir lo dictado por dichas resoluciones. El propio TC ha admitido que las sentencias del TEDH tienen eficacia directa en el ámbito interno[970]. No obstante, el alcance de las decisiones de la institución europea depende íntegramente de los mecanismos que en el ámbito interno se hayan establecido para hacer efectivo lo dictado por aquélla[971]. En el caso del Estado español estos mecanismos están aún por definir y las soluciones planteadas son diferentes[972]. En todo caso, la fuerza real de estas sentencias se descubre no tanto en su posible carácter ejecutivo,

[965] SSTEDH, 24 marzo 1988, Olsson c. Suecia, FJ 66 y siguientes y 7 julio 1989, Gaskin, FJ 42.
[966] LOPERA MESA, *Principio de Proporcionalidad…,* cit., 2006, p. 39. STEDH 10 octubre 2006, L. L. c. Francia, FFJJ 38 y siguientes.
[967] STEDH 22 octubre 1981, Dudgeon c. Reino Unido, FJ 51.
[968] STC 16 diciembre de 1991, FJ 2. SAIZ ARNAIZ, *La Apertura*..., cit., 1999, pp. 158-159.
[969] STEDH 25 de abril 1983, asunto Pakelli, FJ 45; STC, 16 de diciembre de 1991, FJ 2.
[970] STC 25 de octubre de 1993, FJ 8. RIPOL CARULLA, "Incidencia en la Jurisprudencia…", cit., 2007, pp. 311-312.
[971] CARRILLO SALCEDO, *El Convenio*..., cit., 2003, pp. 64-65.
[972] CARRILLO SALCEDO, *El Convenio*..., cit., 2003, p. 71: "En la doctrina española, y ante la insuficiencia de los mecanismos legales disponibles, se han formulado distintas propuestas *de lege ferenda* a fin de resolver el problema jurídico de la ejecución de las sentencias del Tribunal Europeo de Derechos Humanos en el ordenamiento jurídico español: una de estas propuestos, es partidaria de la adopción de una ley *ad hoc,* como el Tribunal Constitucional español sugirió expresamente en su sentencia de 16 de diciembre de 1991 al instar a los poderes públicos a establecer cauces procesales adecuados en orden a la ejecución de las sentencias del Tribunal Europeo de Derechos Humanos; otra, inspirada en la técnica seguida por Noruega o Luxemburgo, propone introducir en las leyes procesales *un nuevo motivo de revisión*; finalmente, una tercera propone introducir *un nuevo motivo de nulidad*."
"La primera de las soluciones propuestas (una *Ley ad hoc*) tiene el inconveniente de la diversidad y heterogeneidad de las distintas soluciones nacionales al problema de los efectos de las sentencias en los sistemas jurídicos de los Estados parte, por lo que sería preferible un Protocolo adicional al Convenio que regulara de modo homogéneo los efectos de las sentencias del Tribunal de Estrasburgo en el Derecho interno de los Estados parte. La segunda (p. 72) (introducir *un nuevo motivo de revisión* en las leyes procesales) podría colisionar con lo esencial de la fundamentación de la especialísima figura procesal de la revisión, pero parece abrirse camino en los autos de la Sala Segunda del Tribunal Supremo, de 28 de diciembre de 2000 y 25 de julio de 2002, y de la Sección Cuarta de la Sala Segunda del Tribunal Constitucional, de 13 de noviembre de 2000, a los que antes me he referido. La tercera, por último (*un nuevo motivo de nulidad o una acción impugnativa autónoma de nulidad*), me parece más fundada y viable ya que podría lograrse a través de la ampliación del artículo 238 de la Ley Orgánica del poder Judicial". LASAGABASTER HERRARTE, *Convenio Europeo*..., cit., 2004, pp. 23-24; RIPOL CARULLA, *El Sistema…,* cit., 2007, pp. 123-127.

sino en su importancia a la hora de interpretar los derechos fundamentales. La interpretación que en estas sentencias se lleva a cabo sobre los derechos fundamentales ha de ser tenida en cuenta necesariamente por los órganos internos encargados de crear y aplicar el derecho. Así lo exige expresamente la propia Constitución española que obliga a interpretar los derechos fundamentales de conformidad con los tratados y acuerdos internacionales firmados por España[973], lo cual se refiere no sólo al Convenio sino también a la jurisprudencia que emana del Tribunal de Estrasburgo[974]. La interpretación de los derechos fundamentales que el TEDH lleva a cabo en la resolución de los conflictos a los que ha de dar solución genera una doctrina a la que se le otorga el efecto de lo que se ha venido en llamar "cosa interpretada"[975]. Se trata de una interpretación con efecto *erga omnes*, no sólo aplicable al caso particular que se resuelve en el asunto concreto, que ha de ser tenida en cuenta en todo caso por los órganos que crean y aplican el derecho a nivel interno[976].

Ciertamente, la aplicación del principio de proporcionalidad por parte de organismos de la envergadura de los tribunales citados, en los que además el Estado español participa, llamaba a la incorporación de dicho principio en el ámbito interno. Sin embargo, esta inclusión necesariamente requería de un fundamento en el ordenamiento interno.

A lo largo del tiempo se han ido estableciendo en el ámbito interno diferentes fundamentos para el principio de proporcionalidad[977]. En el Derecho español al citado principio no le falta base, incluso constitucional[978], para integrarse en el ordenamiento. Así lo ha entendido el TC[979]. El mismo principio de Estado de Derecho[980], que se reconocía en el Derecho alemán como fundamento de la proporcionalidad, o el de justicia[981], constituyen sin duda algunos de los principales pilares sobre los que se basa la proporcionalidad. La necesidad de que el Estado, en sentido amplio, se someta al Derecho en general y a los derechos fundamentales en particular[982], hace que la Administración no pueda en ningún momento con su actuación vaciar de contenido dichos derechos hasta el punto de hacerlos inaplicables[983]. También se ha considerado que la interdicción de la arbitrariedad[984], entendida como límite a los excesos que pueda cometer la Administración[985], y la dignidad, como valor constitucional[986], pueden constituir la base para

[973] Artículo 10.2 CE. SAIZ ARNAIZ, *La Apertura...*, cit., 1999, pp. 52-53 y 205; LASAGABASTER HERRARTE, *Convenio Europeo...*, cit., 2004, p. 21; ARZOZ SANTIESTEBAN, "La relevancia del Derecho…", cit., 2005, pp. 63-64.
[974] ORTEGA GUTIÉRREZ, *Derecho a la Información...,* cit., 1999, p. 98; CATALÁ i BAS, *Libertad de Expresión...,* cit., 2001, p. 39.
[975] RIPOL CARULLA, "Incidencia en la Jurisprudencia…", cit., 2007, p. 311.
[976] SAIZ ARNAIZ, *La Apertura...*, cit., 1999 pp. 143-144; CARRILLO SALCEDO, *El Convenio...*, cit., 2003, p. 63.
[977] BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 600.
[978] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos…,* cit., 1990, p. 51; SÁNCHEZ GONZÁLEZ, "Los límites de los derechos…", cit., 2006, p. 64.
[979] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 333.
[980] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 313; SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p. 116. STC 8 de junio de 1992, FJ 4.
[981] TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, p. 37; ANDRÉS PÉREZ, *El Principio de Proporcionalidad…,* cit., 2008, p. 10.
[982] Artículo 9.1 CE.
[983] NARANJO DE LA CRUZ, *Los Límites...*, cit., 2000, p. 100.
[984] Artículo 9.3 CE. GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 317.
[985] TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, p. 37.
[986] Artículo 10.1 CE.

integrar el principio de proporcionalidad. Su aplicación garantiza en todo caso que, aun limitándose los derechos fundamentales de las personas, quede guardado el valor de la dignidad de las mismas. La proporcionalidad asegura que los límites a los derechos no los dejen vacíos de contenido[987]. La necesidad de que la Administración persiga con objetividad los intereses generales[988] y se someta a los fines que justifican su actuación[989], y la prohibición de que el aparato público actúe de forma arbitraria[990], obligan a que en la actuación de este organismo se aplique el principio de proporcionalidad.

Sin embargo, como ha apuntado algún autor, la principal justificación de que este principio recale en el ordenamiento interno no es otra que la necesidad de dar plena coherencia a un ordenamiento en el que han de convivir bienes jurídicos diferentes que inevitablemente chocarán en situaciones determinadas[991]. La aplicación del juicio de proporcionalidad a la hora de resolver los conflictos entre bienes jurídicos es inevitable. Hay que tener en cuenta que en la búsqueda del equilibrio entre dichos bienes hay que llevar a cabo una tarea de ponderación. Y precisamente en la realización de esta tarea el principio de proporcionalidad constituye un instrumento imprescindible, pues aplica los criterios necesarios para que este juicio pueda resolverse con la solución más justa posible[992].

La incorporación al ordenamiento interno del principio de proporcionalidad se ha asumido por todos los agentes jurídicos. Su aplicación en la actualidad es generalizada y no se discute su empleo como elemento necesario para determinar los parámetros de control de todo límite de los derechos fundamentales.

IIII.2.2. La proporcionalidad como instrumento de control de los límites a los derechos fundamentales.

El juicio de proporcionalidad es un filtro que ha de superar todo límite a un derecho fundamental para que sea admitido por el ordenamiento[993]. Se trata de un instrumento jurídico que evita los excesos a la hora de limitar los derechos fundamentales y que actúa, en este sentido, como herramienta de control de dichos límites[994].

Este principio ha de ser distinguido de otras figuras que en cierta medida determinan también el alcance de los derechos fundamentales y la posibilidad de limitarlos. Se está haciendo referencia a instituciones como el "contenido esencial" de los derechos y la "delimitación" de los mismos, que constituyen figuras dedicadas a configurar el contenido de los derechos y con las que no es difícil confundir el principio de proporcionalidad. No se pretende en este momento

[987] TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, p. 38.
[988] Artículo 103.1 CE.
[989] Artículo 106.1 CE.
[990] Artículo 9.3 CE.
[991] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 341.
[992] DÍEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 115.
[993] STC de 27 de junio de 1990, FJ 8, en el que se reconoce el carácter del principio de proporcionalidad como límite de los límites de los derechos fundamentales. GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, p. 109; BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 216; LOPERA MESA, *Principio de Proporcionalidad...*, cit., 2006, p. 45.
[994] TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, pp. 11-12.

profundizar en el debate creado en torno a las diferencias que caracterizan a cada figura, sin embargo, se plantearán las líneas maestras por donde discurre dicha dialéctica con el fin de situar en sus justos términos el significado del principio de proporcionalidad.

La relación entre contenido esencial y principio de proporcionalidad es clara. La Constitución dispone que el legislador deberá respetar en todo caso el contenido esencial de los derechos y libertades[995]. No obstante, este concepto puede ser interpretado de diversas maneras[996]. En algún caso se ha defendido la que se ha llamado teoría absoluta del contenido esencial. Desde esta perspectiva se podría definir este contenido como conjunto de las "facultades o posibilidades de actuación necesarias para que el derecho sea recognoscible como pertinente al tipo descrito y sin las cuales deja de pertenecer a ese tipo y tiene que pasar a quedar comprendido en otro, desnaturalizándose, por decirlo así", o como "aquella parte del contenido del derecho que es absolutamente necesaria para que los intereses jurídicamente protegibles, que dan vida al derecho, resulten real, concreta y efectivamente protegidos. De este modo, se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección" [997]. Parece que la jurisprudencia identifica aquí un núcleo inamovible y permanente del derecho fundamental que el legislador en todo caso ha de respetar y que se puede reconocer previamente a la actuación de éste[998]. Se afirma, siguiendo la citada teoría absoluta, que el contenido esencial supone un núcleo o ámbito irreductible del derecho fundamental que el legislador no puede alterar y en el que no puede intervenir[999]. Entendido de esta manera el contenido esencial no sería otra cosa que el contenido mínimo sin el cual no puede identificarse un derecho fundamental[1000]. Si una medida vulnerara dicha esfera y sobrepasara sus límites se entendería que atenta contra su contenido esencial. Se constituiría así esta figura como un verdadero límite de límites[1001]. Como se verá, esta forma de entender el contenido esencial ha sido criticada por la doctrina.

Partiendo de la citada teoría absoluta, la consideración de que una medida no es válida porque sobrepasa el contenido esencial de un derecho no se podría distinguir *a priori* claramente de la interpretación de esa medida como desproporcionada. Una medida que atentara contra el contenido esencial de un derecho fundamental podría ser considerada, sencillamente, desproporcionada. Se podrían confundir ambos conceptos[1002]. La distinción según la línea interpretativa expuesta consistiría en reconocer que cada una de las figuras actúa en ámbitos diferentes. El contenido esencial haría referencia a una realidad estable y definida previamente

[995] Artículo 53.1, CE.
[996] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994.
[997] STC 8 de abril de 1981, FJ 8. MARTÍNEZ PUJALTE, *La Garantía*..., cit., 1997, pp. 22-23.
[998] PAREJO ALFONSO, "El contenido esencial…", cit., 1981, pp. 184-186; DE OTTO y PARDO, "La Regulación...", cit., 1988, p. 131; GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, pp. 355-356; SÁNCHEZ GONZÁLEZ, "Los límites de los derechos…", cit., 2006, p. 53.
[999] GARCÍA MACHO, *Reserva de Ley*..., cit., 1988, p. 149; GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 226.
[1000] GARCÍA MACHO, *Reserva de Ley*..., cit., 1988, p. 151.
[1001] PAREJO ALFONSO, "El contenido esencial…", cit., 1981, p. 177; DE OTTO y PARDO, "La Regulación...", cit., 1988, p. 125-127; RODRÍGUEZ-ARMAS, *Análisis del contenido*..., cit., 1996, p. 225.
[1002] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 271.

en cada derecho que, sencillamente, no se podría limitar. La proporcionalidad actuaría en otro ámbito. El reconocimiento de un contenido esencial de los derechos fundamentales intocable llevaría a pensar en la existencia de otro contenido más amplio que no tiene ese carácter esencial. En este segundo ámbito, más amplio, entrarían facultades que pueden ser sacrificadas, al contrario de lo que ocurre con las que componen el contenido esencial[1003]. La limitación de estas facultades tendría que estar sujeta al control de proporcionalidad, por lo que una medida que afectara negativamente a una de estas prerrogativas podría ser declarada desproporcionada a pesar de no afectar al contenido esencial del derecho.

Se entiende aquí que la interpretación que se acaba de exponer sobre lo que es el contenido esencial es de difícil aplicación en la práctica. Por un lado porque la identificación de lo que es el contenido esencial de cada derecho es tarea realmente compleja, y por otro, porque, en la realidad hasta aspectos que en principio se podrían encajar en dicho contenido esencial son limitados. Piénsese en el caso del derecho a la libertad. Si se reconociera que existe un contenido mínimo inamovible del mismo, sería difícil de aceptar que a alguien pudiera negársele esa esfera del derecho. En este sentido, tendría difícil explicación la anulación a las personas presas de su libertad de movimiento[1004]. Ocurre lo mismo con el derecho a la autodeterminación informativa. El TC ha hecho referencia en alguna ocasión al contenido esencial de dicho derecho[1005]. Podría pensarse que reconoce una esfera inamovible del mismo. Sin embargo, la dificultad de configurar un contenido esencial, siguiendo la teoría absoluta, del derecho a la autodeterminación informativa se deja patente en la propia LOPD[1006]. Las múltiples excepciones que se recogen a todas las facultades que componen dicho derecho hacen prácticamente imposible reconocer una esfera en todo caso inamovible e invulnerable. Piénsese en el sector sanitario, donde, como se verá, para llevar a cabo determinadas finalidades, como pueden ser las policiales o la protección de la seguridad pública, prácticamente se anulan las facultades que componen el derecho que se cita. Posiblemente, los únicos criterios imperturbables en relación a esta materia sean, precisamente, los principios de calidad que ahora se están citando. Sin embargo, no en todos los derechos puede reconocerse un ámbito de estas características.

Parece, desde el punto de vista práctico, difícil de encajar el contenido esencial, tal y como se ha entendido hasta ahora, en la realidad. Cosa distinta respecto a este contenido esencial es que el legislador no pueda aprobar una normativa que anule la efectividad de los derechos. Esto no se podrá llevar a cabo no porque exista un contenido imperturbable, sino porque los preceptos constitucionales, también los que reconocen los derechos fundamentales, vinculan al legislador,

[1003] MEDINA GUERRERO, *La Vinculación...,* cit., 1996, pp. 168-170.
[1004] LASAGABASTER HERRARTE, *Las relaciones…,* cit., 1994, p. 386.
[1005] STC 30 de noviembre de 2000, FJ 10: "privada la persona de aquellas facultades de disposición y control sobre sus datos personales, lo está también de su derecho fundamental a la protección de datos, puesto que, como concluyó en este punto la STC 11/1981, de 8 de abril (F 8), <<se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección>>.
De este modo, la LOPD puede ser contraria a la Constitución por vulnerar el derecho fundamental a la protección de datos (art. 18.4 CE), por haber regulado el ejercicio del haz de facultades que componen el contenido del derecho fundamental a la protección de datos de carácter personal prescindiendo de las precisiones y garantías mínimas exigibles a una Ley sometida al insoslayable respeto al contenido esencial del derecho fundamental cuyo ejercicio regula".
[1006] DEL CASTILLO VÁZQUEZ, *Protección de Datos…,*cit., 2007, p. 199.

quien no puede dejarlos sin efecto[1007]. Lo cierto es que los problemas de interpretación que pueden plantearse entre el principio de proporcionalidad y la figura del contenido esencial se resuelven, se entiende aquí, no tanto tratando de distinguir ambas instituciones sino interpretando el contenido esencial en sentido relativo.

Más que en la citada teoría absoluta del contenido esencial se puede pensar en la que se denomina teoría relativa, que considera el principio de proporcionalidad y el de contenido esencial prácticamente como sinónimos[1008]. Según la teoría relativa, el contenido esencial no supone más que la necesidad de justificar el límite que se impone a un bien jurídico a través del juicio de proporcionalidad[1009]. La teoría relativa posibilitaría que en un caso concreto un derecho fundamental viese afectado su supuesto contenido esencial de forma justificada si esta afección estuviera fundamentada en un bien jurídico con fuerza suficiente para ello y superase en ese momento el juicio de proporcionalidad[1010]. Se ha llegado a entender que el contenido esencial no aporta nada nuevo a la teoría de los derechos humanos por cuanto supone, simplemente, la realización de un ejercicio de ponderación[1011]. Desde este punto de vista la regulación que se hace en la normativa referida a la protección de datos tiene mayor sentido. Se reconocen en las leyes una serie de facultades que configuran el derecho a la autodeterminación informativa y estas facultades se limitan dependiendo de las circunstancias y, fundamentalmente, de los fines que se persigan con el tratamiento de datos. Estas limitaciones necesariamente deberán respetar el principio de proporcionalidad para que se guarde un equilibrio entre los diferentes bienes jurídicos que pueden entrar en juego.

Es necesario en este momento aclarar lo que hay que entender por delimitación y limitación, y cómo se incardina el principio de proporcionalidad en el contenido de estas figuras. La confusión entre estos conceptos podría venir de la interpretación que ha realizado una línea doctrinal en relación a esta cuestión. Se ha entendido que los preceptos de la Constitución pueden ser interpretados de tal forma que una vez fijado el contorno de cada derecho fundamental no caben limitaciones sobre los mismos, pues todos estos derechos serán perfectamente compatibles entre ellos sin que puedan entrar en conflicto[1012]. Según esta doctrina el problema de enfrentamientos entre bienes jurídicos no es un problema de límites sino un problema de interpretación de la Constitución[1013]. Los conflictos que se puedan plantear serán meramente aparentes, pues no habrá tal conflicto, sino falta de una adecuada delimitación de uno de ellos[1014]. La delimitación se llevará a cabo interpretando "sistemática y unitariamente" el contenido de la Constitución[1015]. Una vez delimitados, cada derecho fundamental tendrá su

[1007] PAREJO ALFONSO, "El contenido esencial…", cit., 1981, pp. 180-181.
[1008] BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 566.
[1009] MARTÍNEZ PUJALTE, *La Garantía*..., cit., 1997, pp. 20-22; CIDONCHA, *La libertad de empresa…,* cit., 2006, p. 291.
[1010] PRIETO SANCHIS, *Estudios sobre Derechos*..., cit., 1990, p. 151; GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 272.
[1011] DE OTTO y PARDO, "La Regulación...", cit., 1988, pp. 129-130; HÄBERLE, "El legislador…", cit., 1991, pp. 122-123; MEDINA GUERRERO, *La Vinculación*..., cit., 1996, pp. 164-165; BRAGE CAMAZANO, *Los Límites*..., cit., 2004, pp. 399-401.
[1012] MARTÍNEZ PUJALTE, *La Garantía*..., cit., 1997, p. 133.
[1013] DE OTTO y PARDO, "La Regulación...", cit., 1988, p. 135.
[1014] MARTÍNEZ PUJALTE, *La Garantía*..., cit., 1997, p. 133.
[1015] DE OTTO y PARDO, "La Regulación...", cit., 1988, p. 143.

parcela de actuación que no chocará con la parcela de ningún otro. Siguiendo esta interpretación no cabrían limitaciones de los derechos fundamentales ya que su contenido no entraría en colisión con ningún otro bien jurídico[1016]. Así, la aplicación del principio de proporcionalidad no tendría sentido en este momento como instrumento de control de los límites a los derechos fundamentales, pues no habría límite que controlar.

La proporcionalidad y la delimitación se podrían confundir al comprender la delimitación en el sentido anterior, que entiende que tras fijar un contenido definitivo de cada derecho éstos no entran en colisión entre sí. Y es que para poder llevar a cabo esta delimitación y determinar dicho contenido sería necesaria la ponderación entre los diferentes bienes jurídicos. Sólo así se podría encontrar el equilibrio entre todos los bienes jurídicos reconocidos en la Constitución. El legislador, en la labor interpretativa que habría de llevar a cabo a la hora de deducir y concretar el contenido que la Constitución atribuye a un derecho fundamental, necesariamente tendría que ponderar diferentes bienes jurídicos reconocidos en la Ley de leyes. Este ejercicio de ponderación podría confundirse con la aplicación del principio de proporcionalidad, concretamente con uno de sus elementos, como es la proporcionalidad en sentido estricto.

Se interpreta aquí que la figura de la delimitación ha de ser comprendida de distinta manera a la que se acaba de exponer. Cuando se habla de la delimitación de un derecho se hace referencia a la acción de fijar el ámbito que abarca dicho bien jurídico y lo distingue de otros[1017]. Se trata de determinar las facultades que componen un derecho, de concretar su contenido[1018], independientemente de que pueda entrar en colisión con el contenido de otros bienes jurídicos. Este ejercicio de delimitación se lleva a cabo necesariamente partiendo de los preceptos de la Constitución. La Ley de leyes actúa como un todo completo y de su interpretación sistemática tiene que resultar el reconocimiento de diferentes bienes jurídicos que deberán estar definidos y delimitados[1019]. El legislador, y en otra medida el TC[1020], llevarán a cabo una labor interpretativa, un ejercicio de ponderación, a través del que se identificará el contenido de cada derecho. Cuando se aprueban las leyes que entran a regular los diferentes derechos, se determina dicho contenido[1021]. Evidentemente, el margen de actuación del legislador variará dependiendo del enunciado de la Constitución. En derechos en que la Constitución remite al legislador la configuración del derecho sin establecer cuál es su contenido, como es el caso de la autodeterminación informativa, este margen de apreciación será forzosamente más amplio[1022].

[1016] DE OTTO y PARDO, "La Regulación...", cit., 1988, p. 151.
[1017] ALEXY, *Teoría de...*, cit., 1997, pp. 311-312.
[1018] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 72; DÍEZ PICAZO, *Sistema de Derechos...* cit, 2005, p. 107.
[1019] MEDINA GUERRERO, *La Vinculación...,* cit., 1996, pp. 10-13.
[1020] Artículo 5.1 LOPJ: "*La Constitución es la norma suprema del ordenamiento jurídico, y vincula a todos los Jueces y Tribunales, quienes interpretarán y aplicarán las Leyes y los Reglamentos según los preceptos y principios constitucionales, conforme a la interpretación de los mismos que resulte de las resoluciones dictadas por el Tribunal Constitucional en todo tipo de procesos*". MEDINA GUERRERO, *"Artículo 1…",* cit., 2001, p. 78; GARCÍA de ENTERRÍA, *La Constitución…*, cit., 2006, p. 109; LASAGABASTER HERRARTE, *Fuentes del Derecho…,* cit., 2007, p. 42; STERN, *Jurisdicción constitucional…,* cit., 2009, p. 50.
[1021] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 181; MEDINA GUERRERO, *La Vinculación...*, cit., 1996, pp. 90-92.
[1022] MEDINA GUERRERO, *La Vinculación...*, cit., 1996, p. 71.

En la medida en que entra a fijar el régimen jurídico de un derecho, el legislador determinará el contenido normal u ordinario del mismo[1023]. En algunos casos esta tarea no es nada sencilla y lleva a confundir la delimitación con la limitación. Puede ser el caso del derecho a la propiedad[1024]. Por un lado, este derecho se ejerce sobre diferentes tipos de bienes: propiedad intelectual, propiedad sobre el suelo, sobre un vehículo, etc., con lo cuál el régimen deberá acomodarse a las características de cada supuesto y la delimitación del contenido del derecho será diferente en cada caso[1025]. Por otro, la determinación del contenido del derecho a la propiedad es una cuestión compleja debido a que deberá hacerse, según mandato constitucional, atendiendo a la "función social" de dicho derecho[1026]. Esto lleva a que puedan encontrarse frecuentemente medidas que afectan negativamente a la libre disposición de la propiedad pero que no constituyen propiamente una limitación externa del derecho sino su propio contenido ordinario[1027]. No se pretende en este momento analizar la distinción entre estas figuras, sino simplemente subrayar que se entiende necesario diferenciar ambos conceptos, a pesar de los problemas que en la práctica puedan surgir a la hora de llevar a cabo esta tarea.

En el caso del derecho a la autodeterminación informativa la delimitación no plantea problemas de tanta envergadura. Si bien es verdad que el derecho puede ejercerse en diferentes ámbitos, no recae sobre diferentes bienes, de forma que no es necesario crear regímenes distintos que lleven a diferentes configuraciones del mismo derecho. Por otro lado, tampoco se le reconocen a este derecho límites internos, de contenido, que determinen la delimitación del mismo[1028]. Probablemente, el mayor problema que se ha planteado en relación a la delimitación de este derecho ha sido su distinción del derecho fundamental a la intimidad. El contenido tan similar de ambos hace que no sea fácil determinar el ámbito que abarcan. Como ya se apuntara más arriba, en ocasiones se ha discutido incluso la autonomía del derecho a la autodeterminación informativa con respecto a la intimidad. No obstante, tanto el legislador, con la aprobación de la LOPD y anteriormente de la LORTAD, como el TC han acabado por reconocer la existencia del derecho fundamental a la autodeterminación informativa y configurar su contenido.

La delimitación de este derecho se lleva a cabo, como se ha dicho, fundamentalmente por el legislador, aunque también por el TC[1029], que partiendo del artículo 18.4 CE ha delimitado su contenido. El legislador fija de manera meridianamente clara en la LOPD las facultades que componen este derecho: derecho al consentimiento, a la información, al acceso, etc. Esta concreción deriva de la interpretación y armonización que se lleva a cabo de diferentes preceptos de la Constitución, como podrían ser, entre otros, el derecho al libre desarrollo de la

[1023] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 158.
[1024] GARCÍA ENTERRÍA y FERNÁNDEZ, *Curso de Derecho…,* cit., 2004, p. 155.
[1025] LÓPEZ LÓPEZ, *La disciplina constitucional…,* cit., 1988, p. 66; SÁNCHEZ MORÓN, *Derecho Administrativo…,* cit., 2007, p. 693.
[1026] Artículo 33.2 CE: "*La función social de estos derechos delimitará su contenido, de acuerdo con las leyes*". SSTC, 26 de marzo de 1987, FJ 2 ; 17 de marzo de 1994, FJ 4; 20 de diciembre de 2005, FJ 2;.RODRÍGUEZ SANTIAGO, "Las garantías constitucionales…", cit., 2008, p. 176.
[1027] LASAGABASTER HERRARTE, *Las relaciones…,* cit., 1994, p. 365; SÁNCHEZ MORÓN, *Derecho Administrativo…,* cit., 2007, p. 700.
[1028] DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, p. 206
[1029] STC 30 de noviembre de 2000, FFJJ 6,7 y 8.

personalidad[1030], el derecho a la intimidad[1031], la obligación de limitar el uso de la informática[1032] y también de la necesidad de interpretar las normas relativas a los derechos fundamentales y a las libertades de acuerdo con los tratados y acuerdos internacionales firmados por España[1033], entre ellos el Convenio 108/1981 que regula el tratamiento de los datos de carácter personal. Desde esta perspectiva, cuando a los usuarios del sistema sanitario se les reconoce el derecho a la autodeterminación informativa se les están atribuyendo, *a priori*, todas estas facultades que componen el derecho.

La delimitación hay que distinguirla de la limitación. Anteriormente se ha hecho referencia a este ejercicio, que no es otra cosa que excepcionar las facultades que componen un derecho en beneficio de otro bien jurídico[1034]. Es en este momento donde entraría en juego el principio de proporcionalidad. La limitación actúa, en cada caso particular, después de que se haya delimitado el derecho[1035], cuando entre en conflicto con otros bienes jurídicos. No se puede limitar lo que no está definido. Así, una vez se haya determinado el contenido de un derecho puede llevarse a cabo la limitación del mismo. Se trata de límites externos al contenido del derecho. Y es aquí, en este segundo plano, donde se aplica el principio de proporcionalidad, controlando la validez de las medidas que afectan negativamente al derecho[1036]. La delimitación es por lo tanto un *prius* a la aplicación del principio de proporcionalidad[1037].

En la práctica, tanto la delimitación como la aplicación del principio de proporcionalidad constituyen un ejercicio de ponderación, sin embargo, la finalidad en uno y otro caso será diferente. En el primero la ponderación se traducirá en una interpretación por parte del legislador para concretar el contenido de un derecho y en el segundo la ponderación se dirigirá a determinar la validez de una medida que afecta negativamente a dicho derecho.

La LOPD, cuando reconoce el principio de pertinencia, fija la obligación de que toda manipulación de datos supere este juicio de proporcionalidad. Y, como se ha dicho, el respeto a este principio requiere en este ámbito el cumplimiento de dos exigencias. Por un lado, la necesidad de que todo límite externo al derecho a la autodeterminación informativa guarde un equilibrio con el fin que se pretende con su aplicación. En el ámbito sanitario, que es el caso que aquí se analiza, la manipulación de datos de carácter personal no es más que un medio para la consecución de un determinado fin, fundamentalmente garantizar la salud de los ciudadanos. Si se entendiera que para llevar a cabo este fin es necesario exceptuar el derecho de un paciente a consentir un tratamiento de datos determinado, se estaría limitando el derecho a la autodeterminación informativa. El principio de proporcionalidad exige que exista un equilibrio entre el límite que se aplica y la relevancia del bien jurídico que se protege. Por otro lado, el principio de proporcionalidad actúa como límite genérico que afecta a todo tratamiento de datos.

[1030] Artículo 10.1 CE.
[1031] Artículo 18.1 CE
[1032] Artículo 18.4 CE.
[1033] Artículo 10.2 CE.
[1034] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 167.
[1035] MEDINA GUERRERO, *La Vinculación...*, cit., 1996, pp. 20-23.
[1036] MEDINA GUERRERO, *La Vinculación…,* cit., 1996, pp. 93-95.
[1037] GONZÁLEZ BEILFUS, *El Principio de Proporcionalidad...*, 2003, pp. 109-110.

Para proteger la salud de la ciudadanía se entiende necesario recabar y tratar una serie determinada de datos, ni más ni menos. El principio de proporcionalidad actúa aquí como criterio para fijar que los datos a manipular no sean más de los estrictamente debidos. La manipulación de datos afecta al derecho a la autodeterminación informativa de sus titulares. Si bien es verdad que esta afección es difícil de calificar como límite, no es menos cierto que será necesario que se dé, en todo caso, dentro de unos parámetros. Para guardar el debido respeto al derecho a la autodeterminación informativa será necesario encontrar un equilibrio entre la necesidad de proteger la salud de las personas y la necesidad de salvaguardar el derecho de todo ciudadano a controlar el destino de los datos que le conciernen. Este equilibrio parte de la obligación de respetar la regla que establece el principio de proporcionalidad de que no se pueden manipular más datos de los estrictamente debidos en el cumplimiento de un fin.

Otro elemento que se ha confundido en algún caso con el principio de proporcionalidad ha sido el principio de razonabilidad[1038]. Incluso el propio TC emplea en algunos supuestos estos conceptos de manera no suficientemente clara[1039]. Se han llegado a atribuir los elementos que componen el principio de proporcionalidad al principio de razonabilidad. Este último se ha entendido como un juicio en el que han de aplicarse criterios "de pura racionalidad y con ponderación de valores constitucionales"[1040]. Según este último punto de vista el criterio de racionalidad "se proyecta sobre la relación entre los medios empleados por el legislador (...) y los fines que el precepto analizado persigue"[1041]. Así, este análisis que señala al criterio de razonabilidad como elemento que analiza la relación entre medio y fin parece elevar a este principio como sinónimo del de proporcionalidad.

Sin embargo, en la mayoría de los casos el criterio de razonabilidad ha sido definido por parte de la doctrina como un criterio menos exigente que el que aquí se estudia[1042]. No parece que la razonabilidad lleve necesariamente al estudio de los tres subprincipios que componen el principio de proporcionalidad. La razonabilidad exige simplemente que la medida que se adopta para alcanzar el fin no sea "absurda", sino que sea de "sentido común"[1043]. En todo caso, parece claro que una medida que haya superado el juicio de proporcionalidad habrá superado también el de razonabilidad[1044].

III.2.3. Breve referencia a los elementos que componen el juicio de proporcionalidad: adecuación, necesidad y proporcionalidad en sentido estricto.

El juicio de proporcionalidad constituye un análisis de la relación entre medio y fin. Este juicio deberá realizarse una vez se haya resuelto si la finalidad, en sí misma, cumple con los requisitos exigidos por la LOPD. En el apartado anterior se ha estudiado el principio de finalidad fijando los

[1038] APDCM, *Guía de Protección...*, cit., 2004, p. 281; TASCÓN LÓPEZ, *El Tratamiento por la Empresa…,* cit., 2005, p. 88, parecen emplear estos términos de manera aleatoria.
[1039] SSTC, 24 de septiembre de 2007, FJ 6 y 23 de febrero de 2009, FJ 4. SÁNCHEZ GONZÁLEZ, "Los límites de los derechos…", cit., 2006, p. 68,
[1040] STC, 28 de marzo de 1996, voto particular.
[1041] STC, 28 de marzo de 1996, voto particular.
[1042] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 355.
[1043] DÍEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 114.
[1044] AGUADO CORREA, *El Principio...*, cit., 1999, p. 147.

criterios que ha de seguir para que sea acorde a la Ley. El análisis del cumplimiento de estos elementos constituye un examen previo al juicio estricto de proporcionalidad[1045]. Primero se determinará si la finalidad cumple con los requisitos citados y, una vez superado este juicio, se pasará a analizar si se cumple con el principio de proporcionalidad. Así, si el fin no es válido en sí mismo no será necesario ya entrar a valorar la proporcionalidad entre el medio y dicho fin[1046]. Hay quien introduce este análisis dentro del estudio del subprincipio de adecuación[1047]. Sin embargo, se defiende aquí que el análisis del principio de finalidad es previo al de proporcionalidad que afecta a la relación entre el medio que se emplea para alcanzar dicho fin[1048]. En el apartado de la adecuación se pretende establecer la conciliación entre el medio y la finalidad, mientras que en el estudio de la finalidad se analiza la finalidad no en relación al medio sino de forma independiente. Se trata de ver si la finalidad en sí misma cumple con los requisitos necesarios, de concreción y legitimidad especialmente.

Una vez analizada la finalidad se realizará el juicio de proporcionalidad. A la hora de fijar los elementos en los que se va a fundamentar este juicio es un lugar común aceptar que el TC se ha hecho eco a partir de la década de los noventa de lo que la doctrina ha llamado "el *test* alemán de proporcionalidad"[1049]. En base a esta línea de interpretación son tres los elementos que se deben analizar para considerar si un medio es proporcional al fin que persigue: idoneidad, necesidad y proporcionalidad en sentido estricto[1050].

El artículo 4.1 de la LOPD emplea los adjetivos "*adecuados, pertinentes y no excesivos*". Ya se ha dicho en otro lugar que en el Derecho la utilización adecuada de los conceptos es fundamental pues de ello derivan consecuencias jurídicas. Cabe preguntarse cuál es el sentido de cada uno de estos adjetivos. Para algunos autores cada término hace referencia a una realidad concreta, distinta de las demás[1051]. Para otros el empleo de estos términos tiene en esta disposición carácter redundante; se trataría de enfatizar el mismo principio con el uso de términos muy similares[1052]. Lo cierto es que los adjetivos empleados por la Ley podrían corresponderse con el contenido de los criterios que componen el principio de proporcionalidad.

[1045] STC, 22 de marzo de 1991, FJ 3, lleva a cabo un análisis sobre la legalidad y la legitimidad de la finalidad previo al juicio de proporcionalidad.

[1046] GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, pp. 67-69.

[1047] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, pp. 217 y 369; DE LA MATA BARRANCO, *El principio de proporcionalidad…,* cit., 2007, p. 141; BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 694.

[1048] APDCM, *Guía de protección...*, cit., 2004, p. 281.

[1049] SSTC 10 de julio del 2000, FFJJ 6 y 7 y 16 de enero de 2006, FJ 6. LASAGABASTER HERRARTE, *Las relaciones…,* cit., 1994, p. 120; AGUADO CORREA, *El Principio de Proporcionalidad…,* cit., 1999, p. 139; GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, p. 53; BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 334; DE LA MATA BARRANCO, *El Principio de Proporcionalidad…,* cit., 2007, p. 139.

[1050] STC de 16 de diciembre de 1996, FJ 4.

[1051] HERRÁN ORTIZ, *La Violación...,* cit., 1998, pp. 243-244, apunta la posibilidad de que este empleo por parte del legislador de términos con significados similares, no responda a un interés de reforzar una idea, sino que "responde a la necesidad de delimitar y definir realidades diferentes en relación con los datos personales". Considera esta autora que "la adecuación estaría vinculada a la idea de finalidad o calidad del dato recopilado (...) en tanto que la idea de pertinencia se refiere a la cantidad de los datos recopilados, que no se obtengan más datos que los estrictamente necesarios para el fin que se persigue".

[1052] MURILLO DE LA CUEVA, *Informática y Protección...,* cit., 1993, p. 66, señala que a pesar de que es posible atribuir un significado distinto a cada uno de estos términos, no existe "en la ley un uso técnico de las palabras

Se analizarán brevemente los elementos que, en base a lo que la jurisprudencia y la doctrina han afirmado, componen el juicio de proporcionalidad: idoneidad, necesidad y proporcionalidad en sentido estricto. Se trata de criterios que si bien se presentan aquí de forma separada y autónoma tienen diferentes espacios comunes donde interrelacionan e incluso se confunden[1053].

En cuanto a la adecuación o idoneidad, en general, este criterio simplemente requiere que el medio que se emplea se entienda, atendiendo a presupuestos empíricos[1054], como adecuado para la consecución del fin que se pretende. Es decir, se trata de averiguar si a ojos de la realidad conocida, en base a criterios puramente científicos[1055], el medio utilizado puede servir para alcanzar la finalidad perseguida[1056], siempre y cuando el medio sea realizable[1057]. Se habla de *causalidad positiva* entre el medio y el fin, en el sentido de que el medio que se emplea para conseguir el fin ayuda efectivamente a su consecución[1058].

El respeto de la adecuación exige que se cumplan diferentes condiciones. Desde una perspectiva formal se requiere que en todo caso la adecuación esté justificada o fundamentada en alguna norma. La seguridad jurídica exige que el límite al derecho fundamental no sólo sea adecuado en la realidad sino que dicha adecuación esté reflejada y justificada también en alguna norma[1059]. Hay que tener en cuenta que se está hablando de limitar un derecho fundamental. Desde el punto de vista objetivo la adecuación exige que empíricamente el empleo del medio acerque a la finalidad que se pretende[1060]. Y por último, desde el punto de vista subjetivo, se requiere que la limitación al derecho que se lleva a cabo sobre una persona determinada o un grupo de personas determinado se entienda adecuada para llevar cabo el fin[1061]. Es decir ha de haber una relación entre las personas a las que se limita el derecho y el fin pretendido, de tal forma que haya una justificación para que el límite se imponga a dichas personas concretas[1062].

La principal pregunta que se plantea en relación a la adecuación del medio con respecto al fin es si ha de exigirse una máxima adecuación para entender que el medio es idóneo para la consecución del fin. La medida más adecuada será la que con mayor probabilidad y eficacia ayude a obtener la finalidad. ¿Es necesario que la medida a seguir sea la más adecuada para que se entienda que se supera el juicio de proporcionalidad? Se han señalado diferentes posturas en relación a este punto, sin embargo, no parece acertado entender que no es proporcional la medida que no sea la más "idónea". La medida más "idónea" puede tener este carácter pero no pasar los tests de necesidad y proporcionalidad en sentido estricto. Así, en

adecuación y pertinencia que lleve aparejados contenidos distintos. Se trata solamente de una reiteración de ideas con el propósito de recalcar su importancia".

[1053] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 311.

[1054] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos…,* cit., 1999, p. 155; AGUADO CORREA, *El Principio...*, cit., 1999, p 67.

[1055] NARANJO DE LA CRUZ, *Los Límites...*, cit., 2000, p. 103.

[1056] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 220.

[1057] AGUADO CORREA, *El Principio...*, cit., 1999, p. 154.

[1058] LOPERA MESA, *Principio de Proporcionalidad...*, cit., 2006, pp. 387-388; BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 730.

[1059] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 374.

[1060] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 375.

[1061] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos Fundamentales…,* cit., 1990, p. 179.

[1062] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, pp. 375-376.

principio, no hay que descartar una medida por no ser la más adecuada[1063]. No se exige que todos los medios tengan una eficacia absoluta en la consecución del fin, sino simplemente que a través de ellos se pueda obtener el fin perseguido[1064]. Evidentemente, la adecuación es un criterio sujeto a valoraciones, pues una medida puede ser más o menos eficaz para cumplir un fin determinado y por lo tanto más o menos adecuada. Sin embargo, en este momento no se trata de valorar si la medida es más o menos eficaz, sino de considerar si este medio es coherente para llevar a cabo el cumplimiento del fin correspondiente. La inadecuación vendrá cuando el medio sea completamente incoherente para obtener el fin perseguido[1065].

El principio de necesidad se traduce en la realización de un análisis comparativo entre los diferentes medios que podrían llevar a la consecución del fin definido[1066], para acabar concluyendo que el medio empleado en el supuesto concreto es, efectivamente, el menos gravoso pero igualmente eficaz para obtener dicha finalidad[1067]. En este punto no se trata de analizar estrictamente la relación entre medio y fin, sino de hacer una comparación entre los diferentes medios que puedan existir para llevar a cabo el fin, para descubrir si existe un medio menos lesivo para los ciudadanos[1068]. Se trata de averiguar, basándose en criterios empíricos[1069], cuál es entre los diferentes medios adecuados para la consecución del fin, el que menos trastorno supone para el bien jurídico que se sacrifica. La necesariedad implica el tener que emplear el medio más "suave" para proteger de forma efectiva el derecho de que se trate[1070].

Se trata de buscar la medida más eficiente: la que menor coste o sacrificio suponga para el derecho fundamental afectado y que a su vez sea igualmente eficaz en la consecución del fin[1071]. En este parámetro, por lo tanto, hay que analizar tanto la eficacia del medio para conseguir el fin, como la intensidad con la que afecta al bien jurídico sacrificado[1072]. Hay que tener en cuenta que entre diferentes medios a emplear para la consecución de un fin se puede encontrar uno más eficaz que otro pero que, sin embargo, afecta más intensamente al bien jurídico sacrificado[1073]. Así, lo más adecuado puede ser un análisis global de todas las medidas que puedan entrar en juego, atendiendo tanto a la efectividad como al grado de la lesión en el bien jurídico[1074], así como otros factores que pueden también ayudar a decantarse por uno u otro medio, como puede ser el coste económico, la rapidez en la ejecución de la medida, la afección a bienes jurídicos de

[1063] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos Fundamentales…,* cit., 1990, p. 156; LOPERA MESA, *Principio de Proporcionalidad...,* cit, 2006, pp. 388-392.
[1064] NARANJO DE LA CRUZ, *Los Límites...*, cit., 2000, p. 103; TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, p. 22; SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…*, cit., 2004, p. 318; BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 726.
[1065]. GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 303; BERNAL PULIDO, *El Principio de Proporcionalidad…,* cit., 2007, p. 727.
[1066] STC, de 12 de julio 1988, FJ 7.
[1067] GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, pp. 72-77, y pp. 128-129.
[1068] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad...*, cit., 2004, pp. 334-334.
[1069] TERRADILLOS ORMAETXEA, *Principio de Proporcionalidad...*, cit., 2004, p. 25.
[1070] LASAGABASTER HERRARTE, *Las relaciones…,* cit., 1994, p. 120.
[1071] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 305; LOPERA MESA, *Principio de...,* cit., 2006, p. 433.
[1072] LOPERA MESA, *Principio de Proporcionalidad...*, cit., 2006, pp. 436-337.
[1073] BARNES, "Introducción al Principio...", cit., 1994, p. 506.
[1074] LOPERA MESA, *Principio de Proporcionalidad...,* cit., 2006, pp. 439-441.

terceras personas...[1075] Un medio puede ser o no necesario dependiendo de las circunstancias. El TC ha entendido, por ejemplo, que el uso de técnicas de captación de imágenes y sonido por parte del empresario con el fin de controlar a sus trabajadores supera el juicio de necesidad o no, dependiendo de las circunstancias[1076].

Por su parte, el principio de proporcionalidad en sentido estricto conlleva un análisis estrictamente jurídico de la relación entre medio y fin. Se trata de buscar un equilibrio razonable entre los diferentes bienes jurídicos en juego, entre lo que se sacrifica y lo que se persigue con el empleo del medio[1077]. Constituye un juicio ponderativo entre los beneficios que implica la consecución del fin a través del medio empleado, y los sacrificios que supone el uso de dicho medio[1078]. Es el requisito que mayor margen deja a la libre apreciación, pues se trata de valorar la importancia de diferentes bienes jurídicos y del alcance de sus límites[1079].

Este subprincipio trata de analizar desde el punto de vista no ya empírico sino jurídico-valorativo[1080], el peso del bien jurídico que se defiende con el fin que se persigue y el del bien jurídico que se sacrifica con el empleo del medio, para llegar a un equilibrio en el que ninguno de los bienes en juego quede vacío de contenido[1081]. El ejercicio de ponderación, precisamente, supone señalar en un caso determinado y en unas circunstancias concretas cuál de los intereses que colisionan se superpone frente a los demás, si bien, en ningún caso conlleva la desaparición o vaciamiento de los bienes sacrificados, ni supone el establecimiento de una jerarquía con valor permanente para todos los casos entre los diferentes bienes jurídicos[1082]. Se trata de analizar las ventajas y los inconvenientes que derivan de la aplicación del medio adecuado y necesario en la consecución del fin pretendido para llevar a cabo un ejercicio de ponderación razonable entre los mismos[1083]. Como ya ha señalado la doctrina, el principal valor que atesora el ejercicio de ponderación es el hecho de que es un instrumento que dependiendo de las circunstancias que rodean a cada caso particular trae como resultado una solución diferente[1084]. Cuanto mayor sea la afección al bien jurídico limitado en la aplicación del medio, mayor tendrá que ser también la relevancia del bien jurídico que se defiende[1085]. Hay que ver lo que se gana o se pierde con la aplicación o inaplicación del medio.

Si bien en un principio quedan definidos los elementos que componen el juicio de proporcionalidad, lo cierto es que su aplicación por parte del TC no ha sido en numerosas ocasiones todo lo clara que se podía exigir, confundiendo en alguna ocasión los subprincipios y

[1075] LOPERA MESA, *Principio de Proporcionalidad...,* cit., 2006, p. 446.
[1076] SSTC, 10 de abril del 2000, FFJJ 7, 8 y 9 y 10 de julio del 2000, FFJJ 6 y 7.
[1077] GAVARA DE CARA, *Derechos Fundamentales…,* cit., 1994, p. 308; GONZÁLEZ BEILFUSS, *El Principio...*, cit., 2003, pp. 78-83, y pp. 133-134. SSTC, de 17 de febrero de 1998, FJ 8 y 27 de febrero de 2002, FJ 9.
[1078] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos…,* cit., 1990, p. 225.
[1079] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad...*, cit., 2004, pp. 346-347.
[1080] NARANJO DE LA CRUZ, *Los Límites...*, cit., 2000, pp. 108-110.
[1081] BARNES, "Introducción al Principio…", cit., 1994, p. 507.
[1082] DÍEZ PICAZO, *Sistema de Derechos...*, cit., 2005, p. 114; LOPERA MESA, *Principio de Proporcionalidad...*, cit., 2006, p. 545.
[1083] GONZÁLEZ-CUELLAR SERRANO, *Proporcionalidad y Derechos…,* cit., 1990, pp. 231-234; LASAGABASTER HERRARTE, *Las relaciones…,* cit., 1994, p. 120.
[1084] LOPERA MESA, *Principio de Proporcionalidad...,* cit, 2006, pp. 498-499.
[1085] BRAGE CAMAZANO, *Los Límites...*, cit., 2004, p. 223.

no aplicando otras veces alguno de ellos[1086]. Sin embargo, en general, se puede afirmar que este principio crea un sistema de enjuiciamiento de los límites a los derechos fundamentales bastante riguroso que, frente a lo que algunos han afirmado, garantiza la seguridad jurídica a la hora de aplicar dichos límites[1087].

Se ha criticado este criterio debido a que en su aplicación entran en juego valoraciones subjetivas de quienes aplican el derecho, que pueden llevar a dejar en manos de estos últimos la consideración de la relevancia de cada bien jurídico[1088]. Inevitablemente, en el momento en que hay que determinar la relevancia o el peso jurídico de los intereses en juego, quien ha de aplicar en última instancia el principio de proporcionalidad, principalmente Jueces y Tribunales, tendrá en cuenta su criterio. No obstante, esto no quiere decir que la aplicación del criterio de proporcionalidad se vaya a realizar de forma arbitraria, de manera que se genere inseguridad[1089]. Desde algún ámbito se ha tratado de racionalizar, con acierto, la fijación del peso de los bienes jurídicos en juego. Los encargados de aplicar el Derecho han de tener en cuenta en todo momento lo que dicta principalmente la Constitución y las normas que la desarrollan e incluso la interpretan. Hay que ver si, sobre todo en la jurisprudencia, se ha fijado una jerarquía general entre los bienes que en el caso concreto colisionan, en qué medida afecta al bien jurídico en juego la adopción de la medida, de qué manera la adopción de esta medida conlleva la consecución del fin, etc.[1090]

Teniendo en cuenta estos criterios se puede afirmar, que si bien la aplicación del principio de proporcionalidad puede ser criticada por dejar la puerta abierta al uso de criterios subjetivos poco definidos, lo cierto es que es un principio lo suficientemente riguroso como para introducirlo como instrumento de control de los límites de los derechos fundamentales. Realmente, la no aplicación

[1086] BRAGE CAMAZANO, *Los Límites*..., cit., 2004, pp. 335-339.
[1087] BRAGE CAMAZANO, *Los Límites*..., cit., 2004, p. 346.
[1088] BERNAL PULIDO, *El Principio de Proporcionalidad*..., cit., 2007, p. 164.
[1089] LOPERA MESA, *Principio de Proporcionalidad*..., cit., 2006, p. 500.
[1090] LOPERA MESA, *Principio de Proporcionalidad*..., cit., 2006, p. 502: Alexy propone tres elementos para racionalizar esta operación: atender a la intensidad de su afección o satisfacción en el caso concreto; su peso abstracto; y la seguridad de las premisas empíricas que sustentan los argumentos a favor y en contra de la intervención. Estos tres elementos hay que analizarlos: pp. 504: Intensidad de la afectación: "se refiere al grado de afección (o no satisfacción) del principio iusfundamental que se ve restringido por la intervención legislativa (...), así como al grado en que dicha medida contribuye a la satisfacción del principio que respalda la intervención o principio justificante"; p. 514: peso abstracto: "La introducción de esta variable responde pues a la intuición generalizada y plausible de que no todos los principios constitucionales ni, según algunos planteamientos, todas las posiciones de derecho fundamental, tienen la misma importancia desde el punto de vista material". Se puede pensar que en el ámbito de la protección de los datos de carácter personal en el ámbito de la salud, la salud, la integridad física y mental, es más relevante, en abstracto, que la autodeterminación informativa. P. 515: hay que tener en cuenta sin embargo, lo problemático que puede resultar realizar una jerarquía de los derechos fundamentales, en la medida en que en esa tarea entrarían cuestiones puramente morales. p. 525: seguridad de las premisas empíricas: "Con esta variable se mide el grado de certeza acerca de las premisas empíricas que respaldan los argumentos a favor y en contra de la intervención legislativa" (p. 526) "Con su inclusión se pretende dar relevancia al hecho de que no siempre las premisas empíricas con las que se argumenta en torno a la intensidad con que la medida enjuiciada afecta derechos fundamentales o contribuye a la realización de su finalidad cuentan con el mismo grado de certeza, y tal diferencia ha de ser considerada al momento de asignar el peso a cada uno de los principios que intervienen en la ponderación". (...) "Las premisas empíricas favorables a la constitucionalidad de la norma enjuiciada son aquellas que se orientan a probar el *grado de idoneidad* de la intervención legislativa, esto es, la intensidad con que la misma contribuye al logro de su finalidad y, por otro lado, las relativas a la *necesidad* de la medida en razón de la ausencia de alternativas igualmente idóneas y menos restrictivas".

de este principio sí traería como consecuencia directa una mayor arbitrariedad en la fijación de dichos límites[1091].

III.2.4. Aplicación del principio de proporcionalidad en la actuación administrativa.

El principio de proporcionalidad constituye un criterio para definir la validez de los límites a los derechos fundamentales. Este criterio se emplea siempre que entran en juego dichos derechos. El campo de actuación de los mismos es extenso, por lo que la aplicabilidad del principio será también amplia. Hoy día parece reconocerse la eficacia de los derechos fundamentales tanto en las relaciones con los poderes públicos como entre privados[1092]. Es notorio que en las relaciones privadas pueden vulnerarse estos derechos. Piénsese en los conflictos que pueden generarse en el ámbito laboral, que tienen como fondo la violación de derechos fundamentales: igualdad, libertad de expresión, intimidad, entre otros[1093]. No obstante, interesa aquí principalmente el estudio de la proporcionalidad en el campo del Derecho público donde su aplicación presenta características particulares.

Las actuaciones del poder legislativo, del poder judicial y del poder ejecutivo son controlables atendiendo al principio de proporcionalidad. Tanto el primero, aprobando leyes que pueden afectar a la esfera de libertad de los sujetos, como el segundo, en la resolución de conflictos determinados, desarrollan actuaciones que afectan directamente a los derechos fundamentales de los ciudadanos. Esta afección lleva a que el principio de proporcionalidad esté siempre presente en el ejercicio de dichas labores, pues se asegura con su aplicación que la actuación de los citados agentes se realice dentro de unos parámetros, respetando siempre la vigencia de los derechos[1094]. El principio de proporcionalidad establece unos criterios para que dichas decisiones se adopten de forma que los derechos fundamentales se vean afectados en la menor medida posible y siempre de manera justificada.

La Administración, en la medida en que le corresponde la ejecución de las diferentes normas, sean leyes o reglamentos, y en la medida en que su función principal es la de aplicar al supuesto individual lo dispuesto por estas normas, es más susceptible de generar situaciones en las que se limita la esfera jurídica de los ciudadanos, situaciones en que es aplicable el principio de proporcionalidad[1095]. En el ejercicio de las potestades que las normas atribuyen a la Administración, y para alcanzar los fines que el ordenamiento determina que ha de cumplir, las administraciones llevan a cabo actuaciones que necesariamente limitan o afectan a los derechos de los ciudadanos: expropiaciones, denegaciones de licencias, fijación de tasas, imposición de multas, sanciones, etc.

Son múltiples las acciones de las administraciones que afectan negativamente a los derechos fundamentales de los ciudadanos. Precisamente la que se ha llamado actividad limitativa de la

[1091] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, pp. 261-263.
[1092] SSTC, 7 de febrero de 1984, FJ 6 y 10 de octubre de 1988. BILBAO UBILLOS, *La eficacia…,* cit., 1997; GUTIÉRREZ GUTIÉRREZ, *Criterios de eficacia…,*cit., 1999; NARANJO DE LA CRUZ, *Los Límites...*, cit., 2000
[1093] PARDO FALCON, "Los derechos fundamentales…", cit., 1997.
[1094] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p. 212-225; BARNES, "Introducción al Principio…", cit., 1994.
[1095] SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad...*, cit., 2004, pp. 239-259.

Administración[1096] es realmente amplia y puede manifestarse de diversas formas[1097]. Probablemente, el caso más representativo sea el de la actividad policial[1098]. Otro caso claro de afección es el ejercido sobre el derecho de propiedad vía expropiación, que se lleva a cabo tras considerar que el derecho de propiedad incluye también una función social que hace que pueda limitarse a favor del interés público[1099]. Estas actuaciones, para ser acordes a Derecho, necesariamente tienen que superar el juicio de proporcionalidad[1100]. La actuación limitativa de la Administración va, sin embargo, más allá de la actividad expropiatoria o policial: se extiende a situaciones más genéricas, que se reflejan en el funcionamiento diario del aparato público. En lo que aquí interesa, por ejemplo, el derecho a la autodeterminación informativa de los ciudadanos puede verse afectado por el uso constante de las nuevas tecnologías por la Administración. La manipulación de datos de carácter personal, como se ha visto, constituye un ejercicio indispensable en la realización de las diferentes tareas que corresponden al aparato público. Este tratamiento puede limitar el derecho a la autodeterminación informativa de manera contraria a Derecho si no se lleva a cabo dentro de unos parámetros.

Toda actividad administrativa que afecta a los derechos de los ciudadanos ha de cumplir con una serie de requisitos, que garanticen que la afección esté justificada y sea la menor posible. Fundamentalmente, desde el punto de vista sustantivo, es necesario que la finalidad que persiga la Administración tenga unas características concretas y que el medio a emplear en la consecución de dicho fin sea proporcional al objetivo que se persigue.

El primer límite de la actuación administrativa es la necesidad de perseguir en todo caso un interés concreto, que deberá ser además, según mandato constitucional, general[1101]. Ya se ha analizado anteriormente el contenido de la finalidad que configura la protección de la salud. No parece que pueda haber duda alguna sobre la cualidad de esta finalidad como objetivo de interés común. Cuando se habla del interés general se está haciendo referencia al interés colectivo en contraposición al interés privado o particular[1102]. Se trata de la persecución del bien común que representa un interés de la sociedad en su conjunto y que la Administración hace suyo[1103], cuando una norma le atribuye una potestad obligándola a perseguir una finalidad que representa

[1096] VVAA, *Derecho Administrativo*..., cit., 1998, p. 568. "Actividad de limitación, reguladora e imperativa (o de policía): es esta una actividad fundamentalmente jurídica, hecha de normas o de actos de imperio que se imponen coactivamente, de una serie de limitaciones, de condicionamientos o cargas, necesarias para una ordenada convivencia (...)".

[1097] GARCÍA DE ENTERRÍA y FERNÁNDEZ, *Curso de Derecho...,* cit., 2004, p. 106. "la sistematización de supuestos de una incidencia de la actuación administrativa sobre las situaciones jurídicas activas de los administrados (...) puede ser la siguiente; sacrificios de situaciones de mero interés, limitaciones de derechos, delimitaciones administrativas del contenido normal de los derechos, potestades ablatorias (reales, y entre ellas notablemente las expropiaciones), prestaciones forzosas (personales y reales, y entre ellas señaladamente las tributarias), la imposición de deberes y las sanciones".

[1098] AGUADO CORREA, *El Principio...*, cit., 1999, p. 82.

[1099] COSCULLUELA MONTANER, *Manual de Derecho...*, cit., 2006, p. 481.

[1100] BARNES, "Introducción al Principio…", cit., 1994, p. 509; AGUADO CORREA, *El Principio de Proporcionalidad…,* cit., 1999, p. 82; SARMIENTO RAMÍREZ-ESCUDERO, *El Control de Proporcionalidad…,* cit., 2004, p. 201; DE LA MATA BARRANCO, *El Principio de Proporcionalidad…,* cit., 2007, p. 25; ANDRÉS PÉREZ, *El Principio de Proporcionalidad…,* cit., 2008, p. 9.

[1101] Artículo 103.1 CE. SÁNCHEZ MORÓN, *Derecho Administrativo…*, cit., 2007, p.72.

[1102] BLANQUER, *Introducción al...,* cit., 1998, p. 183.

[1103] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 74.

dicho interés[1104]. Así, como se ha dicho por la doctrina y se deduce también de la propia Constitución, el interés general se erige en un auténtico límite a los derechos fundamentales de los ciudadanos[1105]. La Administración tiene la facultad de llevar a cabo actuaciones que limitan los derechos de los ciudadanos cuando se desarrollan a favor de un interés más amplio, colectivo, que se eleva en el caso particular como más relevante que el interés individual de cada ciudadano. En cada supuesto en que la esfera de libertad de la ciudadanía se vea afectada por la actuación de la Administración, será necesario identificar la finalidad de interés general que justifica dicha intervención[1106].

La atribución de potestades a la Administración supone otorgarle la facultad de actuar en diferentes ámbitos de la vida que afectan incluso a los derechos y libertades de los ciudadanos. Estos últimos se ven obligados a soportar las cargas que puedan derivar para ellos de la actuación del aparato público. En cierto sentido se podría decir que el ciudadano queda sujeto en estos espacios[1107] o, como se ha dicho por parte de la doctrina, sometido a lo que la Administración decida dentro de los márgenes que se le han fijado en la potestad atribuida en cada caso[1108]. Se entiende que la pertenencia del individuo a un colectivo social hace que se deban sacrificar en ciertos aspectos sus derechos individuales en beneficio del interés colectivo[1109]. En defensa de dicho interés general el aparato público puede limitar los derechos y libertades de la ciudadanía[1110].

La manipulación de datos por parte de la Administración, cuando se da sin consentimiento principalmente, no estará justificada si no se lleva a cabo con el fin de salvaguardar un interés colectivo, como puede ser la protección de la salud de las personas. La persecución del interés público, por sí misma, no justifica, sin embargo, cualquier actuación de la Administración. No todo vale para el cumplimiento de dicho fin. El tratamiento de la información de carácter personal no podrá realizarse de cualquier manera para el cumplimiento de esas finalidades que representan el interés general. Es aquí precisamente donde entra en juego en la actividad administrativa el principio de proporcionalidad. El cumplimiento de este principio es, por lo tanto, el segundo requisito que ha de respetar toda actuación de la Administración para que sea acorde a Derecho.

Este principio adquiere en el funcionamiento de las administraciones una relevancia significativa. El hecho de que la actividad administrativa limitativa se dirija a perseguir el interés general podría llevar a entender que toda medida adoptada por la Administración queda justificada por sí misma. No obstante, la necesidad de que se respeten los derechos de la ciudadanía obliga a la Administración a llevar a cabo un juicio ponderativo entre los bienes jurídicos en juego en la realización de sus labores, dirigido a encontrar un equilibrio entre los mismos. Esta ponderación se desarrollará teniendo en cuenta los criterios establecidos por el

[1104] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 74.
[1105] BLANQUER, *Introducción al Derecho...,* cit., 1998, p. 185.
[1106] GARCÍA DE ENTERRÍA y FERNÁNDEZ, *Curso de Derecho...,* cit., 2004, p. 62.
[1107] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 447.
[1108] COSCULLUELA MONTANER, *Manual de Derecho...*, cit., 2006, p. 337.
[1109] CARRETERO PÉREZ y CARRETERO SÁNCHEZ, *Derecho Administrativo*..., cit., 1992, p. 74; VVAA, *Derecho Administrativo*..., cit., 1998, p. 591.
[1110] GARCÍA DE ENTERRÍA y FERNÁNDEZ, *Curso de Derecho...,* cit., 2004, p. 104.

principio de proporcionalidad ya citados: idoneidad, necesidad y proporcionalidad en sentido estricto.

El ciudadano aparece ante la Administración pública como sujeto titular de derechos que pueden verse afectados por la actuación de la Administración. El empleo aquí del concepto de "ciudadano" merece un comentario para entender el alcance real de la aplicación del principio de proporcionalidad a una situación; la que se puede reflejar cuando se habla de la protección de datos sanitarios, en la que las personas pueden encontrarse especialmente vinculados a la Administración, en este caso sanitaria.

Se emplea el concepto de ciudadano frente al de administrado para remarcar la situación del individuo con respecto a la Administración pública, no sólo como sujeto pasivo sobre el que recaen las actuaciones de las administraciones, sino también como sujeto activo que ejerce sus derechos frente a éstas[1111]. Es cierto que esta distinción, en la mayoría de los casos, sólo responde a consideraciones meramente ideológicas, ya que en las normas ambos conceptos se emplean en muchos casos de manera indistinta[1112]. Sin embargo, la citada diferenciación parece interesante para resaltar la cualidad de la persona como titular de derechos frente a la Administración.

En efecto, como bien ha apuntado la doctrina, el concepto de administrado refleja sólo parte de esa situación, presentando a la persona como subordinada a la Administración, como sujeto meramente pasivo que parece no ejercer activamente derechos frente a aquélla[1113]. Por el contrario, el concepto de ciudadano es más acorde con la realidad actual y refleja mejor la situación de la persona que se ve afectada por una actuación de la Administración; por un lado, como titular de derechos que la Administración ha de respetar, y por otro, como titular de facultades que el propio ciudadano puede ejercer frente a ésta[1114]. Cierto es que el concepto de ciudadano plantea también algunos problemas de interpretación, sobre todo a la hora de incorporar o no a los extranjeros dentro del mismo[1115]. Sin embargo, en lo que aquí interesa, este concepto resulta más adecuado que el de administrado, más en la actualidad, en la que la denominada Administración electrónica reconoce como uno de sus haberes más importantes la promoción de la participación ciudadana[1116].

Precisamente, en el ámbito de la protección de datos de carácter personal el concepto de ciudadano refleja mejor la situación del titular de los datos. Como se dijera en su momento, la autodeterminación informativa constituye un derecho fundamental que protege a la persona comprendida como sujeto pasivo, englobando acciones dirigidas a garantizar que un agente no entre en el ámbito protegido por este derecho, y también como sujeto activo, abrazando acciones

[1111] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 436.
[1112] EMBID IRUJO, *El Ciudadano...*, cit., 1994, p. 40.
[1113] COSCULLUELA MONTANER, *Manual de Derecho...*, cit., 2006, p. 473.
[1114] GARCÍA DE ENTERRÍA y FERNÁNDEZ, *Curso de Derecho...,* cit., 2004, pp. 15-16.
[1115] EMBID IRUJO, *El Ciudadano...*, cit., 1994, pp. 24-34.
[1116] AIBAR y URGELL, *Estado, Burocracia…,* cit., 2007, p. 193.

positivas que el titular de los datos puede ejercer frente a los otros agentes implicados en el tratamiento de los datos[1117].

El ciudadano, por lo tanto, aparece ante al aparato público como titular de derechos. Sin embargo, hay que tener en cuenta que la relación entre éste y la Administración puede darse en diferentes formas y grados. Evidentemente, y atendiendo al ámbito que se está tratando, no es igual la relación entre la Administración y un ciudadano que aparece en el fichero de la administración sanitaria como un potencial usuario de este servicio y la relación entre la Administración y un ciudadano en tratamiento que está internado en un centro sanitario. La afección a los derechos fundamentales de la ciudadanía puede entenderse que será diferente dependiendo precisamente de dicha relación. En lo que concierne al derecho a la autodeterminación informativa, este derecho se verá afectado con mayor vigor cuando el titular de los datos encuentra una relación más estrecha con la Administración sanitaria.

Cuando la vinculación entre los dos agentes es más estrecha, podría hablarse de las denominadas relaciones "de sujeción especial"[1118]. No se pretende hacer un estudio profundo sobre los problemas que rodean a esta categoría jurídica, sin embargo, cabe hacer un apunte por cuanto que la consideración de una relación como de sujeción especial puede llevar a justificar, por algún sector de la doctrina, una relajación de las garantías en la salvaguarda de los derechos fundamentales de los ciudadanos, entre las que se encuentra el principio de proporcionalidad.

Se pueden considerar las relaciones de sujeción especial como aquellas en que los ciudadanos se encuentran en una situación de especial dependencia frente a la Administración[1119], por la vinculación de gran intensidad que mantienen los dos agentes[1120]. Se ha interpretado por un sector de la doctrina, que precisamente por esta vinculación particular que se da entre los dos sujetos la Administración cuenta con unas prerrogativas, con las que no cuenta generalmente, para limitar los derechos de los ciudadanos que se vinculan de forma especial a ella[1121]. Se trata de entender que frente al *status* común de todo ciudadano hay ciudadanos que por su estrecha relación con la Administración se encuentran bajo un régimen jurídico especial. El ciudadano está generalmente obligado a soportar los efectos de la actuación de la Administración en el ejercicio de sus potestades[1122]. No obstante, se entiende que cuando se produce una vinculación especialmente intensa entre ambos los efectos a soportar pueden ser más gravosos, pues las garantías que protegen sus derechos fundamentales y la aplicación del principio de legalidad pueden verse relajados.

La jurisprudencia no ha mantenido una postura clara respecto a esta figura y lo cierto es que no llega a delimitar con exactitud las situaciones que abraza y los efectos jurídicos que genera. Sin embargo, a lo largo del tiempo ha ido reconociendo cada vez más situaciones dentro de las

[1117] STC 30 de noviembre del 2000, FJ 6.
[1118] GALLEGO ANABITARTE, "Las relaciones especiales…", cit., 1961.
[1119] COSCULLUELA MONTANER, *Manual de Derecho...*, cit., 2006, p. 339.
[1120] GARCÍA URETA, *La Potestad...,* cit., 2006, pp. 56-57.
[1121] LÓPEZ BENÍTEZ, *Naturaleza y presupuestos…,* cit., 1994, p. 161; SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 449.
[1122] LASAGABASTER HERRARTE, *Las Relaciones...,* cit., 1994, pp. 148-149.

relaciones de sujeción especial[1123] y determinando que los principales efectos son la relajación del principio de legalidad que afecta a la Administración y la minoración de las garantías que salvaguardan los derechos de los ciudadanos, que en estos casos se ponen en relación íntima con el aparato público.

Respecto a la legalidad, se ha admitido que este principio puede relajarse en las relaciones de sujeción especial. De esta forma se da al reglamento un mayor protagonismo en la regulación de las materias que afectan a esa relación[1124]. No obstante, la propia jurisprudencia ha admitido que esta relajación en ningún caso puede suponer la deslegalización de materias que han de ser reguladas por la Ley[1125]. En cuanto a la salvaguarda de los derechos fundamentales, la jurisprudencia ha afirmado también que la afección a dichos derechos puede ser mayor en estas situaciones[1126]. Sin embargo, ha subrayado que la existencia de este tipo de relación no puede ser por sí mismo argumento suficiente para despojar a un sujeto de sus derechos[1127].

Las críticas a la figura de las relaciones de sujeción especial y sus efectos son contundentes. En primer lugar, los criterios que regulan la relación entre la Ley y el reglamento no pueden ser alterados por el mero hecho de que se esté ante una supuesta relación de sujeción especial, a no ser que exista una causa justificativa para ello y siempre que se respeten los principios que rigen la citada relación, fundamentalmente la reserva de Ley. Una cosa es que la intervención del reglamento, incluso del reglamento independiente, en algunos supuestos pueda ser mayor, y otra que por el mero hecho de que exista una relación de sujeción especial se alteren los principios que rigen la relación entre la Ley y el reglamento. Y en segundo lugar, afirmar que los derechos fundamentales no tienen vigencia para los ciudadanos que se encuentran en una posible relación de sujeción especial carece de sentido. Los derechos fundamentales, como la propia CE reconoce, vinculan a la Administración[1128]. La mera existencia de una relación de sujeción especial no puede excepcionar la vigencia del derecho fundamental a no ser que la propia CE así lo reconozca[1129].

La realidad es que la existencia misma de las relaciones de sujeción especial ha sido puesta en duda por parte de la doctrina más autorizada[1130]. Es muy complicado dar una definición y unas características comunes a todas las situaciones en que se considera pueden darse las relaciones de sujeción especial[1131], y más complicado aún justificar la limitación de la libertad del ciudadano frente a la Administración simplemente en base a esa supuesta relación más estrecha con la misma[1132]. Dentro de esta categoría jurídica las situaciones que podrían englobarse son heterogéneas y definir unas características comunes para todas ellas es realmente complicado,

[1123] GARCÍA MACHO, *Las Relaciones...,* cit., 1992, p. 212, habla de desmesura en el reconocimiento de situaciones calificadas como relaciones de sujeción especial, pues amplía en exceso el grupo de relaciones que adquieren esa cualidad.
[1124] SSTS, 2 de abril 1991, FJ 2 y 10 de febrero 1997, FJ 4.
[1125] STC 20 de noviembre de 2006, FJ 2.
[1126] SSTC, 19 de julio de 1990, FJ 6 y 17 de enero, de 1991, FJ 2.
[1127] STC 10 de diciembre de 1991, FJ 2.
[1128] Artículo 9.1 CE.
[1129] GARCÍA MACHO, *Las Relaciones...,* cit., 1992, p. 181.
[1130] LASAGABASTER HERRARTE, *Las Relaciones...,* cit., 1994, pp. 425-426.
[1131] GARCÍA URETA, *La Potestad...,* cit., 2006, p. 57.
[1132] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, p. 450.

más cuando de esas características ha de justificarse un régimen de protección de los derechos fundamentales de los ciudadanos más relajado o minorizado[1133]. La jurisprudencia ha señalado también en algún caso que la distinción entre las relaciones de sujeción general y las relaciones de sujeción especial no es nada clara[1134]. Ante esta indeterminación de las fronteras del concepto que ahora se trata, cabe también el riesgo de que esta categoría se extienda llegándose a considerar relaciones de sujeción especial a prácticamente toda relación que se genere entre ciudadano y Administración[1135].

Se entienda o no que este tipo de relaciones existen, lo cierto es que afirmar que por el mero hecho de que una relación entre la Administración y el ciudadano es de sujeción especial los derechos fundamentales de este último pueden verse afectados y limitados por la actuación de la Administración, no parece acertado[1136]. La simple existencia de una relación de sujeción especial no puede constituir argumento suficiente para limitar un derecho fundamental del ciudadano que se relaciona con el aparato público[1137]. La propia jurisprudencia, en algún caso, en supuestos en que los derechos fundamentales de ciudadanos inmersos en una relación de sujeción especial se han visto limitados, ha argumentado que la limitación de dichos derechos deberá basarse en la defensa de otros bienes jurídicos[1138].

La restricción de un derecho fundamental, se dé dentro de una relación de sujeción especial o no, deberá contar con las garantías suficientes, especialmente con la atención al principio de proporcionalidad[1139]. La limitación no vendrá por el hecho de que el titular de los mismos se encuentre inmerso en una relación estrecha con la Administración, sino que estará justificada porque responde a un motivo suficiente que se reconoce en la defensa de un bien jurídico de mayor relevancia.

En lo que aquí concierne, las relaciones entre un paciente y la Administración sanitaria se han podido entender tradicionalmente como relaciones de sujeción especial. Sin embargo, las limitaciones que se puedan imponer al derecho a la autodeterminación informativa de los ciudadanos no vendrán determinadas porque los datos de carácter personal son tratados por la Administración sanitaria en una relación especial con un paciente, sino porque los fines que aquélla persigue defienden bienes jurídicos de especial relevancia como pueden ser la salud pública o la salud individual de las personas[1140]. Desde el punto de vista de la protección de datos de carácter personal, independientemente de que se trate de un ciudadano ingresado en un centro sanitario o no, lo relevante a la hora de determinar el régimen que seguirá el tratamiento de sus datos será en todo caso la finalidad que se persiga con la manipulación de la información. Así, deberá atenderse a la relación entre los datos que se manipulan y cómo se manipulan, y la finalidad que se persigue para justificar un tratamiento determinado de los datos.

[1133] LASAGABASTER HERRARTE, *Las Relaciones...,* cit., 1994, p. 418.
[1134] STC 8 de junio de 2001, FJ 4.
[1135] GARCÍA URETA, *La Potestad...,* cit., 2006, p. 59.
[1136] COSCULLUELA MONTANER, *Manual de Derecho...*, cit., 2006, p. 340.
[1137] LASAGABASTER HERRARTE, *Las Relaciones...,* cit., 1994, p. 415.
[1138] STS 17 de julio 2006, FJ 5.
[1139] LASAGABASTER HERRARTE, *Las Relaciones...,* cit., 1994, pp. 413-414 .
[1140] SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2006, pp. 450-451.

III.3. El principio de proporcionalidad en el tratamiento de datos de carácter personal sanitarios.

Todas las consideraciones que se han realizado sobre el contenido y el sentido del principio de proporcionalidad o pertinencia han de ser aplicadas ahora al caso concreto que en este trabajo se trata, que no es otro que el de la manipulación de datos de carácter personal por la administración sanitaria con el fin de salvaguardar la salud. Como se ha dicho al comienzo de este apartado, el principio de proporcionalidad puede ser analizado en el ámbito de la protección de datos desde dos perspectivas: como instrumento para controlar los límites que se quieran imponer al derecho a la autodeterminación informativa y como regla general que ha de cumplir todo tratamiento de datos. Las particularidades que presenta la aplicación de este principio desde la primera perspectiva se irán analizando a lo largo de este trabajo, en la medida en que se estudien los límites a las diferentes facultades que componen el derecho a controlar los datos que conciernen a cada uno: derecho a ser informado, a otorgar el consentimiento, etc. Todos estos límites deberán superar el juicio de proporcionalidad que se ha propuesto. Merece la pena ahora centrarse en la segunda perspectiva, que expresamente recoge la LOPD y que obliga a que en todo tratamiento de datos la información que se manipule sea proporcional en relación a la finalidad que se persigue.

IIII.3.1. La adecuación de los datos recogidos para la finalidad sanitaria perseguida.

En los diferentes apartados que se han analizado ha quedado suficientemente justificado que la manipulación de datos, en general, constituye una medida adecuada para conseguir el fin que ahora se pretende, que no es otro que la protección de la salud de las personas[1141]. No hacen falta mayores argumentos para darse cuenta de que el tratamiento de los datos sanitarios se erige en un medio fundamental e imprescindible para llevar a cabo ese objetivo. En el primer capítulo se argumentó que la información constituye, para el correcto funcionamiento de la sanidad, un instrumento indispensable. Planes como los ya citados eEuropa, impulsado por la UE[1142], o el Plan Avanza[1143], vigente en el Estado español, apuntan como una de sus principales preocupaciones la de crear un sistema de información efectivo. En el ámbito autonómico el último Plan Estratégico de Osakidetza reconoce también como uno de sus principales retos la implantación de un sistema de información avanzado[1144]. La asistencia directa a los pacientes requiere, como es lógico, una base sólida de información veraz y actual para que sea llevada a cabo con el mayor éxito posible. El tratamiento de una enfermedad oncológica, por ejemplo, exige el conocimiento no sólo de información estrictamente médica, sino de información relacionada con los hábitos de vida del paciente. Qué decir de las enfermedades transmisibles por contagio como el VIH. La investigación en el sector médico y la realización de estadísticas exige también, evidentemente, la manipulación de información sobre la que basarse. Los estudios epidemiológicos que analizan las causas, características y consecuencias de las epidemias requieren también de la manipulación de los datos que puedan aportar información

[1141] RUIZ CARRILLO, *El Tratamiento de los Datos…,* cit., 2008, p. 35.
[1142] http://europa.eu/, en la sección referida a la sociedad de la información.
[1143] http://www.planavanza.es/
[1144] Plan Estratégico 2003/2007 de Osakidetza, p. 62, en http://www.osanet.euskadi.net/.

sobre estos elementos. La realización de estadísticas necesita también, como es obvio, de datos. La actuación para hacer frente a las situaciones que ponen en riesgo la salud pública requiere igualmente de información sobre la que trabajar. Incluso las acciones judiciales que puedan derivar de las actuaciones en el ámbito de la sanidad exigen para su resolución de información que describa los hechos que han llevado a generar el conflicto en cuestión. Resumiendo, prácticamente toda actuación que se quiera llevar a cabo en el sector sanitario requiere para su realización la manipulación de datos, de una gran cantidad de información.

Sin embargo, lo que en este momento plantea el subprincipio de adecuación no es si el tratamiento de datos, en general, es idóneo para el cumplimiento de un fin. Plantea una exigencia más concreta. Se trata del análisis de si la manipulación de cada uno de los datos que se pretenden tratar constituye un medio adecuado para llevar a cabo los fines que el ordenamiento ha dispuesto que la Administración sanitaria tiene que cumplir, independientemente de si es necesario el consentimiento del titular de la información o no. Algún informe jurídico de la AEPD ha resaltado la importancia del criterio de adecuación como parámetro a tener en cuenta para determinar la validez de un tratamiento de datos. Haciendo referencia a una historia clínica en la que se recogía el dato de si el paciente iba en su automóvil con el cinturón de seguridad puesto en un momento determinado, señala que este dato no es adecuado para llevar a cabo la finalidad de tratar al paciente con fines sanitarios, con lo que no se cumple con el principio de proporcionalidad o pertinencia[1145]. Cosa distinta sería si el fin fuera, por ejemplo, en caso de haber habido un accidente, imponer una sanción administrativa a dicho sujeto por incumplir la normativa de tráfico.

Como se ha dicho, el subprincipio de adecuación requiere de un análisis desde diferentes puntos de vista. Desde un punto de vista objetivo se trata de ver si, atendiendo a criterios científicos y desde una perspectiva puramente empírica, el tratamiento de todos los datos de carácter personal que se quieren manipular constituye un medio adecuado para la salvaguarda de la salud. Al analizar el principio de finalidad se ha visto que el ordenamiento determina una serie de objetivos hacia los que la Administración sanitaria tiene que dirigir, en todo caso, su actividad. Pues bien, según este criterio la recogida y manipulación de todos y cada uno de los datos tiene que ser adecuada para el cumplimiento de dichos fines. Hay que ver si realmente existe una relación de causalidad positiva entre la manipulación de la información vinculada a personas determinadas y la consecución de los fines. Tiene que quedar claro, por parte del responsable del fichero, que el tratamiento de todos los datos constituye un medio apto para llevar a cabo el fin que en cada caso concreto se quiere alcanzar[1146]. Necesariamente, si los datos que se recogen van a estar destinados al cumplimiento de un fin determinado, el respeto al derecho a la autodeterminación informativa exigirá que sólo puedan recabarse y tratarse los datos que estrictamente se estimen adecuados para alcanzar dicho fin.

Piénsese en el caso en que un paciente acude al médico de cabecera con los síntomas de una gripe. En un inicio, será adecuado recabar y manipular determinados datos para poder tratar dicha enfermedad: cuándo comenzó a padecer los síntomas, si tiene fiebre, las circunstancias en

[1145] Informe Jurídico de la AEPD, 0173/2008, 26 de marzo del 2008.
[1146] SANTOS GARCÍA, *Nociones Generales...*, cit., 2005, p. 53

que ha podido llegar a enfermar, si las personas allegadas o cercanas padecen los mismos síntomas… Toda esta información superará en mayor o menor medida el juicio que propone la adecuación desde la perspectiva objetiva, en la medida en que es información idónea para lograr el objetivo, que no es otro que tratar al paciente y restablecer su salud. Si bien algunos datos pueden ser más adecuados que otros, la manipulación de todos ellos lleva a la consecución del fin. Existe una relación de causalidad positiva entre medio y finalidad. Sin embargo, imagínese que para tratar esa misma enfermedad se solicita información sobre la orientación sexual del paciente. Evidentemente, los datos concernientes a esta realidad no superarán el citado juicio, pues su recogida y tratamiento no es un medio adecuado para conseguir el fin. El uso de esta información no aporta nada desde el punto de vista científico para lograr el objetivo. La manipulación de esta información no lleva empíricamente a la consecución del fin, por lo que es un medio inadecuado y, por lo tanto, no supera el juicio de proporcionalidad.

Desde una perspectiva subjetiva hay que ver si es adecuado recoger y tratar los datos de determinadas personas identificadas o identificables con el objetivo de salvaguardar la salud de la ciudadanía. Hay que analizar si en el supuesto concreto existe una relación entre la persona que verá su derecho a la autodeterminación informativa afectado y la finalidad que se persigue, es decir, si está justificado el tratamiento de los datos de dicha persona concreta para el cumplimiento del fin. En el campo de la sanidad este extremo plantea ciertas particularidades. Normalmente, cuando la manipulación de los datos se dirige a realizar un servicio a una persona concreta, estos datos se vinculan a dicha persona determinada. Es decir, cuando una finalidad se relaciona con una persona, normalmente los datos a tratar se referirán a ella. Ejemplo de ello es el ámbito bancario, o el laboral, en los que la gestión de determinados bienes o la situación laboral de una persona determinada requieren de la manipulación de los datos referidos a dicha persona concreta. En estos casos, como en la mayoría, la identidad del titular de los datos se corresponde con la identidad de la persona a la que va dirigida la actuación que requiere la manipulación de los datos. Por el contrario, en el ámbito sanitario la salvaguarda de la salud puede requerir de datos no sólo del paciente puntual sino también de sus familiares u otras terceras personas. La adecuación, por lo tanto, plantea en este caso un problema de cierta entidad. Se trata de ver si con el fin de proteger la salud de una persona pueden ser tratados los datos de terceros. Piénsese en las enfermedades contagiosas en las que el conocimiento de actuaciones de terceros puede ser importante a la hora de tratar la enfermedad de un paciente, o en el caso de los datos genéticos que por su propia naturaleza contienen información compartida entre diferentes personas.

No se trata de ver en este momento cómo se resuelve el choque entre el derecho a la salud de una persona y la intimidad de una tercera que puede verse afectada precisamente con el fin de proteger la salud de esa persona. Esta cuestión será analizada al hablar del consentimiento. Lo que se trata de ver es si el tratamiento de los datos de una tercera persona puede constituir un medio adecuado para la salvaguarda de la salud de otra persona. La respuesta debe ser afirmativa. Evidentemente, habrá que atender a cada caso. Sin embargo, la premisa de la que ha de partirse no es otra que la que posibilita, siempre atendiendo a criterios científicos, que datos de terceras personas sean tratados para la salvaguarda de la salud de los ciudadanos.

Por último, desde el punto de vista formal, se trata de ver si una norma posibilita que los datos de carácter personal sean manipulados por la Administración sanitaria para la salvaguarda de la salud. No es necesario llevar a cabo ahora un análisis ponderativo entre el bien jurídico que se ve afectado, el derecho a la autodeterminación informativa, y el bien jurídico que se trata de proteger, que no es otro que la salud de las personas. Este ejercicio de ponderación se llevará a cabo en el subprincipio referido a la proporcionalidad en sentido estricto. Ahora sólo se trata de ver si una norma abre la posibilidad de que determinados datos puedan ser manipulados para obtener el fin que se pretende.

La propia LOPD reconoce expresamente esta posibilidad[1147]. Sin embargo, no determina qué datos en concreto se pueden manipular en cada caso. Sería absurdo pensar que una Ley orgánica puede entrar a regular una materia hasta ese punto de detalle. En última instancia son los reglamentos los que determinarán con mayor o menor concreción qué datos podrán emplearse para llevar a cabo cada finalidad concreta. En este sentido, la LOPD exige que las normas que crean los ficheros públicos señalen la estructura básica del fichero y la descripción de los tipos de datos que se van a manipular[1148]. Por ejemplo, la norma que crea determinados ficheros del Servicio vasco de salud habilita en el fichero denominado Detección Precoz del Cáncer de Mama a los profesionales para manipular datos identificativos, DNI, nombre y apellido, dirección, teléfono; datos de características personales: fecha y lugar de nacimiento, sexo; datos de circunstancias sociales: aficiones y estilo de vida; datos especialmente protegidos: salud[1149]. Con la manipulación de estos datos se pretende coordinar el programa de prevención del cáncer de mama, realizar las citaciones de las participaciones en el programa, gestionar los flujos de información y evaluar los resultados del programa[1150].

La adecuación, desde el punto de vista formal, quedaría cubierta con esta previsión. Podría ser discutible el que se incluya alguna de esas categorías en la norma, dando por hecho que se trata de información adecuada para lograr el fin descrito. También puede ser criticable el hecho de que se empleen conceptos tan genéricos como el de "estilo de vida". No obstante, hay que recordar que la adecuación no exige la máxima adecuación. Un dato no será adecuado para conseguir un fin sólo si se demuestra que su manipulación no va a llevar de ninguna manera a la consecución del fin. No hay que olvidar, además, que con la superación del requisito de la adecuación una manipulación no se erige en proporcional, siendo imprescindible pasar el filtro de la necesidad y el de la proporcionalidad en sentido estricto. Es por ello que el uso de cláusulas genéricas puede estar justificado.

La adecuación del tratamiento de una serie de datos en relación a un fin sanitario concreto deberá analizarse, por lo tanto, atendiendo a estas tres previsiones. En caso de que se entienda

[1147] Artículo 7.6 LOPD.

[1148] Artículo 20.2 LOPD: "*Las disposiciones de creación o de modificación de ficheros deberán indicar: (...) d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo*".

[1149] Punto 4.3.d) del Anexo II, Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

[1150] Punto 4.3.a) del Anexo II, Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio vasco de salud.

que este juicio es superado se pasará a analizar los subprincipios de necesidad y proporcionalidad en sentido estricto.

III.3.2. La necesidad de la recogida de datos y su tratamiento.

Este subprincipio exige un análisis comparativo, partiendo de criterios empíricos, entre los diferentes medios que pueden emplearse para la consecución de un mismo fin, para tratar de descubrir cuál de todos ellos es el que conlleva la realización satisfactoria de dicho fin sacrificando en la menor medida posible el derecho en juego. En algún informe jurídico la AEPD ha planteado el juicio de necesidad como criterio principal para resolver un conflicto en relación a la posibilidad de emplear determinados datos con un fin concreto. Se trata de la posibilidad de utilizar una fotografía en la tarjeta identificativa de los trabajadores de una empresa. Se plantea la agencia si es posible cumplir con el fin identificativo empleando otra medida. Llega a la conclusión de que no cabe encontrar una medida menos gravosa con el derecho a la autodeterminación informativa e igual de eficiente, resolviendo que se trata de un medio necesario[1151]. En el ámbito que se está estudiando habrá que ver si es necesario el tratamiento de determinados datos de carácter personal para llevar a cabo las actuaciones dirigidas a la salvaguarda de la salud de los ciudadanos.

Por lo visto hasta este momento no parece descabellado afirmar que el tratamiento de datos de carácter personal, en general, es un medio no sólo adecuado, sino también necesario para proteger la salud de la ciudadanía. Se podría afirmar que el tratamiento de datos de carácter personal es una actividad inherente, más allá de necesaria, a la realización de las acciones que comprenden la salvaguarda del derecho a la protección de la salud. Y es que no es fácil imaginar alternativa alguna a la manipulación de los datos de carácter personal para cumplir los mismos fines. Lo que ahora hay que analizar, sin embargo, es qué criterios hay que seguir para concluir si la manipulación de determinados datos es necesaria para llevar a cabo esos objetivos.

Dentro de la información que puede ser considerada como adecuada para cumplir dichos fines podrán encontrarse datos que por sus características no son necesarios manipular. Si el tratamiento de unos datos lleva a la consecución del fin pretendido, aunque sea de forma lejana, pero afecta de manera especialmente gravosa a la autodeterminación informativa y hay otros datos que llevan de forma más eficiente a la realización del objetivo, incluso afectando igual al derecho a la autodeterminación informativa, se entenderá que la manipulación de la primera información no será necesaria, pues existe otra información que lleva de manera más eficiente a la consecución del objetivo. Piénsese en el caso en que a un sujeto afectado por la gripe se le solicita información sobre el estilo de vida familiar. La manipulación de estos datos podría resultar empíricamente idónea para tratar la enfermedad, debido a que la enfermedad podría haber sido causada por hechos relacionados con esas circunstancias. Esta información resultaría adecuada. No obstante, no parece que sea necesario conocer dicha información para tratar la enfermedad citada. El uso de dichos datos afectaría directamente a la autodeterminación informativa, e incluso a la intimidad del paciente y de su familia; en cambio, su efectividad para tratar la

[1151] Informe de la AEPD, 266/2006.

enfermedad sería mínima, pues en general se puede tratar esa enfermedad sin que sea preciso conocer esa realidad, atendiendo a otros datos sanitarios.

El subprincipio de necesidad plantea diferentes cuestiones. En primer lugar, lleva a tener que analizar si, debido a las características del fin que se persigue en el ámbito sanitario, puede estar justificada la recogida y tratamiento de datos que aparentemente podrían no ser necesarios. Este principio ha sido empleado en alguna resolución para considerar un tratamiento de datos contrario a Derecho. Se trataba de un centro sanitario que transmitió a una empresa más información de la debida en el justificante de una baja laboral. Concretamente, el centro incluyó en dicho justificante información sobre los problemas psicológicos que el trabajador había tenido, sin que dichos datos fueran necesarios para cumplir el fin pretendido[1152].

Una de las cuestiones más relevantes que plantea este subprincipio en el ámbito sanitario es la cantidad de datos que ha de ser recogida para llevar a cabo estas finalidades. La necesariedad plantea la duda de si en el tratamiento de un paciente concreto o en la realización de una actividad de las que se han citado en el apartado dedicado a la finalidad, será necesario recoger todos los datos posibles que puedan ser empleados en dicha actividad independientemente de que luego, en la práctica, sean manipulados o no. Es decir, cabe preguntarse si ante la duda de que la manipulación de unos datos determinados sea o no necesaria, cabe su recogida. Se plantea la posibilidad de que haya datos excesivos que vayan a ser objeto de manipulación[1153].

De inicio, el principio de pertinencia exige que la recogida de cada uno de los datos que va a ser manipulado sea necesaria[1154]. El Grupo de Trabajo del artículo 29 de la Directiva ha subrayado en algún caso la obligación de cumplir con el principio de proporcionalidad en este sentido. Entrando a valorar, por ejemplo, la proporcionalidad de una decisión marco del Consejo relativa al uso del registro de nombres de determinados pasajeros con el fin de luchar contra el terrorismo, concluye este grupo que si bien la finalidad perseguida es relevante, el citado principio exige que se haya de buscar un equilibrio entre el objetivo y el derecho fundamental a la autodeterminación informativa. Esto implica que deberán limitarse los datos que se vayan a recabar con dicho fin, pues el daño que causa su uso es excesivo con respecto a los resultados que se obtienen[1155].

En el ámbito sanitario en muchas ocasiones la posibilidad de concretar los datos que se estiman necesarios para conseguir la protección de la salud es mínima. Durante un proceso sanitario puede surgir la necesidad de hacerse con nuevos datos. Las normas de creación de los ficheros de la Administración deben concretar los datos que han de recogerse para la consecución de los fines que se pretenden[1156]. En el ámbito sanitario, sin embargo, en la mayoría de los casos esta identificación de los datos se lleva a cabo con cláusulas genéricas que otorgan

[1152] Resolución AEPD, R/00977/2008, 22 de julio de 2008, procedimiento AP/00010/2008.
[1153] RUIZ CARRILLO, *Manual Práctico…,* cit., 2005, p. 23.
[1154] ALMUZARA ALMAIDA, "Relaciones Precontractuales…", cit., 2007, p. 149.
[1155] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre la "Propuesta del Consejo relativa al uso del registro de nombres de pasajeros a efectos de la aplicación de la Ley presentado por la Comisión el 6 de noviembre de 2007", adoptado el 5 de diciembre de 2007.
[1156] Artículo 20.2.d) LOPD.

a los responsables de los ficheros un margen bastante amplio a la hora de recoger la información. Si se atiende por ejemplo al fichero relativo al registro de los casos de SIDA de Osakidetza se verá que se recogen datos de muy diverso tipo, que se refieren a distintos aspectos de la vida de las personas afectadas[1157]: desde datos de carácter meramente identificativo hasta datos relativos a la vida sexual, estilo de vida y aficiones del sujeto en cuestión. Cláusulas como "estilo de vida" dan el citado margen de maniobra a los responsables del fichero que pueden tener la duda de si todos los datos que se refieren a dicho "estilo de vida" son necesarios para llevar a cabo los fines que se pretenden en torno a la enfermedad del SIDA: tratamiento médico, investigación epidemiológica, estudios estadísticos, etc.

Evidentemente, el profesional sanitario en el ejercicio de su tarea, en la que las variables son innumerables, tendrá dudas sobre la necesidad o no de determinada información. Lo cierto es que dicho profesional no puede estar constantemente preguntándose sobre lo necesario o no del tratamiento de cierta información, pues ello constituiría un obstáculo en el ejercicio de su labor. Hay que tener en cuenta que el principal bien jurídico a proteger en este sector es especialmente relevante en la mayoría de los casos. Esta consideración lleva a afirmar que, ante la duda de que la recogida y manipulación de unos determinados datos sea necesaria o no, parece recomendable apostar por una postura flexible que posibilite su tratamiento siempre y cuando la decisión se tome en base a criterios médicos[1158]. Es por ello por lo que el uso de cláusulas más o menos genéricas a la hora de señalar qué datos cuyo tratamiento puede ser adecuado para la consecución del fin puede estar justificado. En este sentido parece haberse decantado también la jurisprudencia[1159]. La selección entre todos estos datos que se consideran adecuados de los que se considerarán necesarios la realizará el profesional sanitario atendiendo al caso concreto.

Se ha comentado más arriba que en este ámbito la manipulación de la información es una actividad fundamental y que una de las claves del buen funcionamiento del sistema sanitario es la creación de un eficiente sistema de información. Por ello, cuando se habla del principio de pertinencia aplicado al ámbito sanitario, hay que puntualizar que hay que entenderlo como criterio que obliga a recoger los datos estrictamente necesarios para la asistencia, pero todos los que son necesarios. El artículo 15 LBAP reconoce la necesidad de que la HC recabe los datos necesarios para llevar a cabo el tratamiento sanitario del paciente[1160]. La referencia a los datos necesarios parece que abraza todos los necesarios. El profesional sanitario ha de disponer en cada momento de toda la información necesaria para llevar a cabo su trabajo. La necesidad que impone el principio de calidad de que sólo se pueda tratar la información "adecuada, pertinente y no excesiva" no puede constituir una barrera para que esta labor se lleve a cabo de la mejor forma posible. Es decir, el principio de pertinencia no puede suponer, en ningún momento, un obstáculo para que los profesionales sanitarios recojan y traten los datos que estimen necesarios

[1157] Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de Salud.
[1158] TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 407, advierte que en el ámbito sanitario es necesario recabar más datos que en otros ámbitos para prestar una adecuada asistencia.
[1159] STSJ de Galicia 24 de septiembre de 2008, FJ 4.
[1160] Artículo 15.1 LBAP: "*La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente (…)*".

para llevar a cabo su labor[1161]. Un excesivo recelo en la defensa del derecho a la autodeterminación informativa e intimidad no debe afectar al correcto tratamiento sanitario.

El profesional ha de contar con "toda" la información necesaria para establecer un diagnóstico y un tratamiento determinado[1162]. Si en un momento dado la cantidad y heterogeneidad de los datos a recapitular ha de ser grande, el principio de proporcionalidad, y en general el derecho a la autodeterminación informativa, no puede suponer un obstáculo para llevar a cabo esta manipulación de los datos[1163]. No obstante, con todo ello no se quiere decir que el profesional sanitario tenga carta blanca para requerir y manipular arbitrariamente los datos que quiera. Lo que se plantea es que en la relación de confianza que ha de existir entre profesional y paciente el primero no tenga problemas para acceder a toda la información que estime necesaria para llevar a cabo el tratamiento adecuado, o la investigación o tarea pertinente.

En segundo lugar, una interrogante que podría plantear el subprincipio de necesidad es el saber si es o no necesario que los datos aparezcan asociados a una persona identificada o identificable. La disociación es un proceso que se recoge expresamente en la propia LOPD[1164] y que hace que unos datos no puedan ser vinculados a su titular. La cuestión referente a la disociación es importante, pues los datos que no pueden ser vinculados a una persona determinada o determinable, identificada o identificable, no serán considerados como información de carácter personal por lo que no les será aplicable la Ley, al no conllevar su tratamiento riesgo alguno para el derecho a la autodeterminación informativa de los ciudadanos[1165]. Ya se ha comentado cuándo se entiende que una persona se considera identificada o identificable a efectos de aplicar la Ley.

Se podría pensar que el empleo de datos disociados por los profesionales sanitarios constituye una alternativa en la realización de sus tareas. Sin embargo, es evidente que en la mayoría de supuestos, principalmente en el tratamiento médico, es imprescindible que los datos se vinculen a sus titulares. La asistencia sanitaria directa a pacientes determinados requiere de información vinculada a esas personas concretas. En el caso de las acciones judiciales derivadas de la asistencia sanitaria ocurre lo mismo: la información a emplear en un proceso judicial determinado, vinculado a una actividad asistencial concreta, deberá estar asociada a personas determinadas. Los estudios epidemiológicos requieren también, en la mayoría de los casos, de la vinculación de los datos con determinadas personas que se hayan visto afectadas por la enfermedad correspondiente, pues, por mucho que al final pueda tratarse de casos en los que se vean implicadas numerosas personas, el estudio de la epidemia requerirá del análisis de las características particulares de cada caso. En estos supuestos, en realidad, el tratamiento de los datos de manera no asociada no es una alternativa, pues la asociación resulta absolutamente

[1161] APDCM, *Guía de Protección...,* cit., 2004, p. 116, apunta que el "principio de calidad debe interpretarse no como limitativo en cuanto al número y tipo de datos que pueden utilizarse, sino como promotor de un criterio de racionalidad en el manejo de la información". P. 282: Así pues, señala esta Agencia que, para "prestar determinados servicios sociales es posible que sea necesario recabar gran cantidad de datos de una persona, y de muy variado tipo, no debiendo entenderse que la protección de datos limita el número de datos a tratar".
[1162] SOLERNOU VIÑOLAS, "Aspectos Legales...", cit., 2006, p. 57
[1163] APDCM, *Guía de Protección...*, cit., 2004, pp. 281-282.
[1164] Artículo 3.f) LOPD.
[1165] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, p. 33. SAN 8 marzo 2002, FJ 5.

necesaria. Por lo tanto, no se estará ante diferentes posibilidades que se pueden comparar, sino ante un medio que hay que ver si es adecuado o no para la consecución del fin. Se entiende aquí que esta cuestión es previa al análisis del subprincipio de necesidad y que afecta al de adecuación. Lo que habrá que ver es si el tratamiento de los datos disociados es un medio adecuado para llevar a cabo las actividades citadas. Ya se ha dicho que para muchas operaciones que componen el fin de la protección de la salud no lo es, pues la manipulación de estos datos disociados no lleva en la práctica a la consecución del fin.

No obstante, sí hay supuestos en que la disociación constituye una alternativa real al tratamiento de datos de carácter personal. Los casos que más dudas pueden plantear son los de la investigación y realización de estadísticas. En estos últimos supuestos, no parece que sea necesario vincular esos datos a una persona concreta. En el caso de las estadísticas, no es requisito indispensable, ni mucho menos, que los resultados se muestren asociados a personas determinadas o determinables. La elaboración de estadísticas basándose en datos que parten de ficheros de cualquier sistema sanitario no requiere de la utilización de datos vinculados a personas identificadas o identificables. En este sentido, parece que es una alternativa no sólo adecuada y aconsejable, sino necesaria, que dichos resultados se muestren disociados, pues para cumplir el fin de la estadística no es imprescindible esa vinculación. Con la investigación ocurre algo parecido. Para llevar a cabo trabajos de investigación, en muchos casos, no será necesario que los datos aparezcan vinculados a personas determinadas o determinables.

En estos supuestos, el empleo de datos asociados a una persona determinada o determinable lleva a la consecución del fin. Sin embargo, el mismo fin se hace efectivo también con el empleo de los mismos datos pero de manera disociada. Esto hace que la utilización de información disociada supere con mayor éxito el juicio de necesidad. El medio que cumple el mismo fin afectando en menor medida el derecho a la autodeterminación informativa evidentemente constituye un medio más “necesario” que el medio que cumple el fin de igual manera pero afectando de forma más gravosa el citado derecho.

Aplicando el criterio de necesidad se determinará, por lo tanto, qué datos entre los que se estiman adecuados pueden, por ser su uso preciso, emplearse. Habrá que atender al caso concreto para concluir, en base a criterios científicos, qué información es la necesaria. Pero este juicio deberá realizarse en base a parámetros meridianamente laxos, pues lo contrario podría llevar a entorpecer la labor del profesional sanitario.

IIII.3.3. La proporcionalidad en sentido estricto entre los datos recogidos y la finalidad sanitaria perseguida.

En lo que corresponde a la proporcionalidad en sentido estricto, lo que hay que observar es si desde el punto de vista jurídico, no fáctico, la manipulación de los datos de carácter personal está justificada para llevar a cabo las diferentes actuaciones que se han citado: asistencia sanitaria, investigación epidemiológica, salvaguarda de la salud pública, etc., que constituyen fundamentalmente los fines a perseguir. No se trata de un elemento puramente formal como el que se veía al analizar el subprincipio de adecuación, que exigía ver si una norma reconoce la posibilidad de emplear un medio para alcanzar un fin concreto. Consiste en llevar a cabo, en un

caso determinado, un análisis de ponderación entre la relevancia jurídica de los bienes jurídicos en juego, para ver si puede sacrificarse el derecho a la autodeterminación informativa a favor de la salvaguarda de la salud de los ciudadanos.

En términos generales consiste en analizar la colisión entre los diferentes bienes jurídicos que podrían entrar en conflicto en la manipulación de datos de carácter personal en el ámbito sanitario. No se trata de establecer una relación jerárquica definitiva entre los intereses en juego, sino de determinar en un caso concreto qué bien jurídico prevalece sin que ello suponga un vaciamiento del contenido de cualquiera de ellos. La búsqueda del equilibrio en este choque es el objeto de la aplicación de la proporcionalidad en sentido estricto. No es, ni mucho menos, una cuestión sencilla, pues la casuística en este ámbito es muy amplia y las variantes numerosas. Como se verá a lo largo de este trabajo, sobre todo al analizar los límites a las diferentes facultades que componen el derecho a la autodeterminación informativa, son varios los bienes jurídicos que entran en juego. Se trata de ver, en cada caso, si el bien jurídico que defiende o representa el fin correspondiente justifica la manipulación de datos de carácter personal, además, en la mayoría de casos que se analizarán, sin el consentimiento del titular. Hay que remitirse a los apartados en que se analiza el consentimiento, el derecho a ser informado, la cesión de datos, etc. para estudiar de forma detenida las confrontaciones entre los diferentes bienes jurídicos en juego.

Más allá de este análisis genérico, lo que exige este subprincipio es el estudio del choque entre los derechos que se han citado en cada supuesto concreto de tratamiento de datos. Deberá determinarse si la protección de la salud, como bien jurídico, justifica que una información concreta sea manipulada, atendiendo a la afección al derecho a la autodeterminación informativa que conlleva. No consiste en realizar un estudio científico para ver qué medida es necesaria, sino en verificar si es razonable desde el punto de vista estrictamente jurídico el sacrificar el derecho a la autodeterminación informativa de la manera en que se ha de sacrificar en el caso concreto para favorecer o promocionar el derecho a la protección de la salud.

Piénsese, por ejemplo, en el supuesto en que se quiere llevar a cabo una investigación científica, en que se pretenden manipular datos sanitarios sin el consentimiento del titular, con el fin de probar un determinado fármaco contra la gripe. Más allá de que esta manipulación pueda ser adecuada y necesaria, es evidente que de ninguna manera superaría el juicio de proporcionalidad estricta. La afección al derecho a la autodeterminación informativa es significativa y el beneficio que se produce a favor de la protección de la salud no especialmente importante. No hay equilibrio alguno desde el punto de vista jurídico.

Tratándose de un análisis estrictamente jurídico no parece que tengan que ser los profesionales sanitarios quienes deban llevar a cabo este juicio valorativo. Estos profesionales han de tener el marco jurídico definido a la hora de desarrollar su actividad, de tal forma que tengan claro cuándo, cómo y para qué pueden emplear los datos de carácter personal de sus pacientes. Al estar afectados derechos fundamentales ha de ser el legislador, cuando menos de inicio, quien basándose en el marco constitucional ha de concretar claramente cuales son los fines que justifican la manipulación de los datos de carácter personal.

La LOPD, fundamentándose en lo que plantea la propia CE, dispone una solución genérica: el derecho a la autodeterminación informativa cede, en gran medida, cuando se trata de proteger la salud. En estos casos se limita el derecho del titular a consentir el tratamiento de unos datos cuando la finalidad sea la salvaguarda de la salud[1166]. Tanto las actuaciones que van encaminadas a proteger la salud individual como colectiva pueden llegar a justificar, cuando sea necesario, la manipulación de los datos de carácter personal sin el consentimiento del titular de los mismos. Ya se justificó la posibilidad de que el interés colectivo se constituya en límite al derecho a la protección de datos de carácter personal. La jurisprudencia también así lo ha reconocido[1167]. La prevalencia del derecho a la autodeterminación informativa podría suponer la imposibilidad de tratar datos de carácter personal, por lo menos sin el consentimiento del titular, lo cual, en última instancia, podría ir en detrimento de la salud de la ciudadanía. Ya se ha visto en el apartado referente a la finalidad, que el derecho a la protección de la salud constituye un bien jurídico de suficiente entidad para poder limitar el derecho fundamental a la autodeterminación informativa.

Sin embargo, la cesión de este derecho frente a la protección de la salud no es absoluta, no hay un vaciamiento del primero. Según la Ley no cualquier tipo de tratamiento de datos vale para salvaguardar la salud de los individuos. La propia norma exige que el sacrificio de este derecho fundamental se dé sólo con ciertas garantías, principalmente el respeto a los principios de calidad y la adopción de las medidas de seguridad oportunas. Así pues, según la Ley, el derecho a la autodeterminación informativa cede a favor del derecho a la salud siempre y cuando se respeten ciertos parámetros que aseguran que el derecho sacrificado quede afectado en la menor medida posible. Ya se dijo al analizar el sentido del principio de proporcionalidad que uno de sus haberes era precisamente que conllevaba un equilibrio coherente entre los bienes en juego sin que se pudiera llegar a vaciar el contenido de alguno de ellos. La Ley fija un marco jurídico general ideal para que los datos de carácter personal puedan ser tratados con la finalidad de salvaguardar la salud.

El problema que se plantea en la LOPD con respecto a este punto es que el marco jurídico que define es excesivamente amplio y genera cierta inseguridad jurídica. Atendiendo a la Ley, los profesionales sanitarios saben que pueden tratar datos de carácter personal para salvaguardar la salud de sus pacientes. Sin embargo, a la hora de llevar a cabo operaciones concretas en el día a día se generan dudas, pues no se establece para qué casos se pueden emplear unos u otros datos sanitarios.

Evidentemente, una Ley orgánica no puede entrar a analizar todos estos matices. La LOPD plantea una solución genérica y una posibilidad, la de poder tratar los datos referentes a la salud de una persona para salvaguardar precisamente su integridad física y mental. A partir de esta premisa el ordenamiento deberá concretar los diferentes aspectos que entran en juego en la manipulación de datos en el ámbito de la salud. Y es que el juicio de proporcionalidad estricto se da en cada operación de tratamiento de datos. Cada acceso, cada cesión, cada cancelación, ha de estar justificada. En esta línea la LBAP pretende establecer las líneas maestras de cómo ha

[1166] Artículo 7.6 LOPD.
[1167] STSJ Comunidad de Madrid 10 de abril de 2003, FJ 9.

de manipularse la historia clínica. Sin embargo, tampoco alcanza a resolver todos los problemas que presenta la variada casuística que se da en este ámbito. Como se dijera más arriba, la LBAP no llega a concretar con todo el éxito posible el contenido de la Ley de protección de datos en el ámbito sanitario. Parece que la resolución de los conflictos que puedan generarse en cada caso, cuando se manipula información sanitaria, se ha de encontrar en las ya citadas normas de creación de ficheros.

IV. EL PRINCIPIO DE VERACIDAD.

En el ámbito de la protección de datos de carácter personal el principio de veracidad es probablemente el que menos problemas ha planteado. Si se analiza la doctrina que ha tratado esta materia se verá que este principio en concreto no ha dado pie a grandes debates[1168]. Lo cierto es que la exigencia que reconoce la LOPD a este respecto no deja lugar a la ambigüedad ni plantea grandes problemas de interpretación. No obstante, esta circunstancia no es óbice para que se resalten una serie de puntos sobre el principio de veracidad, que ayuden a comprender mejor las exigencias que derivan del mismo.

IV.1. Significado y contenido del principio de veracidad.

IV.1.1. Definición del principio de veracidad.

En primer lugar hay que destacar la importancia de este principio. A pesar de no haber suscitado grandes polémicas, el principio de veracidad reconoce una exigencia de gran relevancia, que la propia jurisprudencia ha resaltado en alguna ocasión[1169].

Se ha dicho que todo tratamiento de datos de carácter personal ha de perseguir una finalidad determinada. Pues bien, desde un inicio, para cumplir o alcanzar esa finalidad mediante la manipulación de datos es necesario que la información a tratar no sea inexacta, falsa, incompleta, o no actualizada. Los datos erróneos, incompletos o pasados, como se verá, dificultan que se cumpla satisfactoriamente la finalidad perseguida. El principio de veracidad evita que se puedan manipular este tipo de datos y , por lo tanto, se eleva como requisito indispensable para la realización efectiva de las finalidades pretendidas.

El respeto al principio de veracidad resulta necesario para proteger el derecho a la autodeterminación informativa. La manipulación de datos erróneos irremediablemente afecta negativamente a la autodeterminación informativa. El control sobre la información que afecta a las personas pasa porque los datos no-veraces sean destruidos o rectificados. Hay que tener en cuenta, además, que el uso de estos datos puede afectar también a otros derechos. La manipulación de información errónea sobre las personas puede traer consigo efectos perjudiciales para éstas. Piénsese, por ejemplo, en el daño que puede causar el uso de datos no-veraces en el ámbito sanitario. De esta manera, este principio constituye también una regla de relevancia en el respeto al derecho a la autodeterminación informativa y otros derechos.

[1168] SANZ CALVO, "Calidad de los datos…", cit., 2008, p. 154.
[1169] SAN 28 de junio 2002, FJ 3.

La exigencia de cumplir con el principio de veracidad se reconoce expresamente en la Ley de protección de datos. En un primer pronunciamiento la LOPD requiere que, en su tratamiento, los datos reflejen en todo momento, con exactitud y actualidad, la realidad a la que se refieren[1170]. En un segundo paso, la Ley exige que, en caso de que los datos no respondan a la realidad exacta, completa y actual, estos datos falsos, inexactos, incompletos o pasados sean sustituidos por los rectificados y completos[1171]. Y finalmente, a la hora de regular las medidas de seguridad a adoptar en el tratamiento de los datos, recoge la necesidad de que el responsable del fichero y el encargado del tratamiento, en la medida que le corresponde, adopten todas las medidas necesarias para que el principio de veracidad se haga efectivo y se garantice en todo momento la integridad de los datos[1172]. El reglamento que desarrolla la Ley recoge esta regulación y la completa señalando cómo ha de llevarse a cabo la actualización de los datos por parte del responsable o, en su caso, encargado del fichero[1173]. Estas disposiciones siguen en términos generales los criterios establecidos por la Directiva europea. Señala esta norma, recogiendo lo que disponía el Convenio de 1981[1174], que los datos deberán ser exactos y actualizados, cuando sea necesario, debiendo tomarse las medidas oportunas para que la información inexacta o incompleta sea suprimida o rectificada[1175].

Llevando a cabo una lectura conjunta de esta normativa parece clara la exigencia que plantea el principio de veracidad. Se requiere que, en todo caso, los datos que se vayan a tratar para la consecución de cualquier finalidad sean exactos, actualizados y completos. Si bien en un inicio este planeamiento no presenta demasiados problemas, lo cierto es que a la hora de aclarar el contenido del principio se encuentra algún que otro punto oscuro.

[1170] Artículo 4.3 LOPD: "*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado"*.

[1171] Artículo 4.4 LOPD: "*Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16"*.

[1172] Artículo 9 LOPD.

[1173] Artículo 5.5 RDLOPD: "*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.*

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviere el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento".

[1174] Artículo 5 Convenio 108/1981 del Consejo de Europa.

[1175] Artículo 6.1 Directiva 95/46/CE: "*Los Estados miembros dispondrán que los datos personales sean:*

c) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados".

Como ha puesto de manifiesto la doctrina, los conceptos de actual, exacto, completo y veraz, pueden llegar a confundirse y a superponerse los unos a los otros[1176]. Lo exacto hace referencia a lo puntual, fiel y cabal[1177], en relación con la realidad que se pretende reflejar en el dato. Es decir, el dato es exacto cuando refleja lo que el emisor del mismo quiere reflejar y es reconocido por el receptor de la misma manera[1178]. Lo completo, por su parte, se refiere a lo lleno[1179]. No parece que con ello se exija que cuando se quiera reflejar una realidad haya que aportar todos los matices sobre la misma, sino que basta con que la información que se aporta sea la suficiente como para reconocer e identificar dicha realidad. Actual hace referencia al tiempo presente[1180], de tal forma que cuando se exige que los datos sean actuales se requiere que se refieran al tiempo en el que se tratan, y no al pasado. Y lo veraz se refiere a lo que es real, a lo no falso[1181]. Como se ha dicho, todos estos elementos pueden llegar a confundirse entre sí. Por ejemplo, en la mayoría de los casos lo exacto requerirá que la información sea completa[1182] y actual[1183], pudiendo, también, el último concepto englobar a los otros dos.

Ciertamente, y si bien atendiendo a los significados de los términos utilizados puede resultar redundante la redacción de la LOPD, queda suficientemente claro cuál es el requerimiento que hace el legislador. Con el principio de veracidad se exige que el responsable del fichero incluya y mantenga los datos recogidos de forma exacta, completa y actualizada. Independientemente de que los datos se recaben del propio titular, a través de cesión o vía fuentes accesibles al público, el principio de veracidad reclama una actuación suficientemente diligente por parte del responsable del fichero para que los datos reflejen en todo momento, fielmente y de forma actualizada, la realidad que se refiere al titular de la información.

IV.1.2. Un apunte sobre la necesidad de que los datos sean actualizados y la necesidad, en determinados casos, de conservar los datos del pasado.

La LOPD exige que los datos reflejen la situación actual de la realidad a la que se refieren. Se deduce de este precepto que en todo momento la información que se trata de manipular deberá ser actualizada. Si se comparan esta norma y la anterior Ley reguladora de protección de datos se observará una pequeña diferencia que, sin embargo conlleva efectos jurídicos de importancia.

La Ley anterior exigía que los datos respondiesen a la situación "real" del afectado[1184]. Atendiendo a este requerimiento los datos tenían que reflejar la realidad del titular de los datos, sin embargo, no se fijaba si esa realidad debía referirse a situaciones del presente o del pasado. Por el contrario, la Ley ahora en vigor exige que los datos respondan a la situación "actual",

[1176] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 26.
[1177] http://www.rae.es/
[1178] RUIZ CARRILLO, *Manual Práctico...*, cit., 2005, p. 20; RUIZ CARRILLO, *El Tratamiento...,* cit., 2008, pp. 34 y 35.
[1179] http://www.rae.es/
[1180] http://www.rae.es/
[1181] http://www.rae.es/
[1182] http://www.rae.es/, como sinónimos del vocablo "cabal" se utilizan las palabras completo y exacto.
[1183] RUIZ CARRILLO, *Manual Práctico...*, cit., 2005, p. 26.
[1184] Artículo 4.3 LORTAD: "*Dichos datos serán exactos y puestos al día de forma que respondan con veracidad a la situación real del afectado*".

además de real, de dicho ciudadano. La jurisprudencia ha entendido que "lo real es lo que tiene existencia verdadera y efectiva y lo actual lo que sucede en el tiempo presente"[1185]. Lo real, por lo tanto, no tiene por qué ser actual, sino que puede referirse a una realidad ya pasada. Pues bien, la actualidad de los datos se plantea en la vigente Ley como requisito indispensable para el cumplimiento del principio de veracidad[1186].

El motivo por el que se lleva a cabo el cambio en la redacción de la norma es claro. El hecho de que en la Ley anterior se exigiese simplemente que los ficheros respondiesen a la situación real del afectado, causaba incertidumbre pues daba pie a que se pudieran mantener ficheros no actualizados[1187]. Si los datos simplemente debían reflejar la situación real del titular de los mismos, no la situación actual, se considerarían admisibles los ficheros que contuvieran datos que reflejasen la situación pasada del titular. Esta posibilidad ha de ser de partida rechazada por el ordenamiento. Si bien es cierto, como se verá, que en determinados sectores es necesario conservar datos concernientes a realidades pasadas para tener una perspectiva histórica de la realidad actual, como norma general se puede afirmar que los datos que reflejan el pasado difícilmente podrán ser útiles para perseguir una finalidad determinada en el presente[1188]. Y los datos que no son necesarios para llevar a cabo la finalidad que se persigue con la manipulación han de ser cancelados, pues su tratamiento afectaría innecesariamente de manera negativa al derecho a la autodeterminación informativa. Hay que recordar que, en base al principio de pertinencia, sólo se pueden manipular los datos estrictamente necesarios para alcanzar el fin que se pretende conseguir. La Ley anterior habilitaba al responsable del fichero para que pudiera mantener ficheros con datos del pasado. Es por ello por lo que el cambio en la redacción de la Ley está plenamente justificado.

Esta cuestión ha sido analizada por la jurisprudencia en el estudio de los ficheros que contienen datos que reflejan el llamado "saldo cero"[1189]. En estos supuestos el dato refleja la situación de una persona que ha sido incluida en un fichero de solvencia patrimonial por no haber pagado una deuda cuando debía, pero que, sin embargo, la ha saldado, aunque extemporáneamente, más adelante[1190]. El dato de "saldo cero", por lo tanto, indica que una persona incumplió en cierto momento una obligación, pero que más adelante pagó la deuda atrasada. Ciertamente, el citado dato responde a la verdad, refleja una situación real. No obstante, no se puede decir que refleje una situación actual, pues se refiere a que en el pasado un individuo incumplió una obligación. El mantenimiento en el tiempo de un dato como el citado, que refleja una situación sucedida en el pasado, sólo puede tener la finalidad de etiquetar a las

[1185] SAN 12 de mayo de 2004, FJ 3.
[1186] APDCM, *Manual de Datos...*, cit., 2003, p. 25, advierte que "la desactualización puede afectar a la veracidad y se corre el riesgo de que el afectado sea tratado en forma desigual respecto de los demás ciudadanos". (...) "No son pocos los que opinan que un dato desactualizado es un dato falso".
[1187] Los principales problemas se han desarrollado en el ámbito bancario con los conocidos ficheros de morosos, en los que era frecuente la aparición de nombres de personas que en un pasado fueron morosas pero que ya habían saldado sus deudas. Así, la propia SAN 12 de mayo de 2004, o la SAN 24 de marzo de 2004, SAN 3 de marzo de 2004, SAN 7 de junio de 2004. TRONCOSO REIGADA, "El principio de calidad…", cit., 2010, p. 358.
[1188] VELÁZQUEZ BAUTISTA, *Protección Jurídica…,* cit., 1993, p. 126.
[1189] ALMUZARA ALMAIDA, "Relaciones Precontractuales…", cit., 2007, p. 157; ALMUZARA ALMAIDA, "Ficheros Privados…", cit., 2007, p. 486.
[1190] SAN 7 de junio 2002, FJ 2.

personas de forma injustificada, lo cual ha de ser rechazado por el ordenamiento. Se trata de señalar de forma indirecta y sin justificación alguna que una persona fue morosa en algún momento[1191]. Mantener un dato que refleja la morosidad del pasado es no recoger la situación real y actual del individuo afectado y, por lo tanto, vulnera el principio de veracidad[1192]. En la LOPD este escollo queda salvado y, en todo caso, los datos deberán mostrar la realidad actual[1193].

El requerimiento de que los datos reflejen en todo caso la realidad actual se ha puesto de manifiesto, también, en el litigio sobre la actualización de los ficheros bautismales. Algunas personas pretendieron que de los ficheros eclesiales desapareciera su condición de bautizados. Querían dejar de aparecer en dichas bases de datos debido a que ya no pertenecían a la Iglesia católica. Los tribunales decidieron que la Iglesia no tenía la obligación de cancelar los datos de estas personas debido a que éstos no configuraban un fichero y, por lo tanto, no les era aplicable la LOPD[1194]. Más allá de que estas bases de datos puedan ser consideradas ficheros o no[1195], lo cierto es que el litigio generado en relación a los ficheros bautismales resulta interesante desde el punto de vista del principio de veracidad.

Este principio exige que la información refleje en todo caso la realidad actualizada de los titulares de la misma. Siendo esto así, el mantenimiento de los ficheros bautismales sin actualizar lleva a que se conserven datos que reflejan una realidad pasada no cierta: que unos sujetos que ya no pertenecen a la Iglesia católica siguen vinculados a la misma[1196]. El respeto estricto del principio de veracidad debería llevar, se entiende aquí, a que los datos se tuvieran que actualizar para reflejar la realidad presente. Las bases de datos de la iglesia deberían recoger el hecho actual de que las citadas personas han dejado de pertenecer a la iglesia. La solución acorde al estricto cumplimiento del principio de veracidad podría consistir en la cancelación de los datos. El respeto a dicho principio exige que no se guarden o mantengan datos del pasado en la medida en que no son pertinentes para el cumplimiento de la finalidad perseguida. Podría pensarse también que, de acuerdo a criterios históricos y estadísticos, y al igual que ocurre en el Registro Civil con la anotación de la nulidad, separaciones y divorcios al margen de la inscripción de los matrimonios[1197], bastaría para cumplir con la veracidad la mera anotación en el fichero de la voluntad de abandonar su condición de bautizado. Así, los ficheros responderían a la realidad actual sin necesidad de cancelar y suprimir dato alguno, de forma que esta información pudiera seguir siendo empleada con fines estadísticos e históricos. En un inicio, así lo entendió la AEPD en sendas resoluciones que resolvieron esta cuestión antes de que llegara a tribunales. Se obligaba a la Iglesia a realizar una anotación en el margen del libro bautismal señalando la

[1191] SAN 31 de mayo 2002, FJ 3; SAN 10 de mayo 2002, FFJJ 4 y 5.
[1192] SAN 7 de junio 2002, FJ 3.
[1193] GARRIGA DOMÍNGUEZ, *La Protección...*, cit., 1999, p. 179
[1194] STS 19 de septiembre de 2008; SAN 22 de octubre de 2008.
[1195] MESSÍA DE LA CERDA BALLESTEROS, "El Derecho a la Protección…", cit., 2007, p. 230, "no parece existir dificultad alguna en afirmar la consideración e los libros bautismales como un supuesto de fichero".
[1196] MESSÍA DE LA CERDA BALLESTEROS, "El Derecho a la Protección…", cit., 2007, Pp. 234-236, realiza un interesante análisis en este sentido; ARENAS RAMIRO, "La Sentencia del Tribunal Supremo…", cit., 2008, p. 219, aboga por la posibilidad de cancelar los datos.
[1197] Artículo 76, Ley 8 de junio de 1957, sobre el Registro Civil.

voluntad de los sujetos citados de suprimir su condición de bautizados[1198]. Si bien el criterio de la agencia no abogaba por la cancelación de los datos, planteaba una solución intermedia que acercaba al cumplimiento del citado principio. Sin embargo, esa solución fue rechazada también por los Tribunales en una decisión muy criticada por diferentes sectores[1199].

La necesidad de que, por exigencia del principio de veracidad, los datos reflejen esta realidad actual plantea varias cuestiones a resolver. En primer lugar, cabe preguntarse si es posible admitir casos en los que se puedan conservar datos que reflejan la realidad del pasado. Parece indiscutible que en algunos supuestos puede resultar útil, para la defensa de bienes jurídicos de alto interés, como puede ser la salvaguarda de la salud, mantener datos que reflejan la situación pasada del ciudadano. Efectivamente, en determinadas situaciones puede entenderse justificada la conservación de datos del pasado de forma que su cancelación puede no ser apropiada[1200].

La propia LOPD reconoce la posibilidad de conservar los datos del pasado en la medida en que su manipulación sea necesaria para cumplir la finalidad que se persigue[1201]. En el ámbito sanitario parece claro que para proteger la salud de las personas puede ser necesario tener una perspectiva histórica de la evolución de la salud de cada paciente, para lo cual será imprescindible conservar durante un plazo razonable los datos del pasado. En este campo la normativa sanitaria exige que los datos no sean cancelados automáticamente aunque hayan sido actualizados. La supresión de los datos contenidos en las historias clínicas no se llevará a cabo, según dispone la LBAP, hasta transcurrido un período mínimo de cinco años desde la fecha del alta de cada proceso asistencial[1202].

Más allá del sector sanitario, en muchos otros casos puede ser también útil mantener archivos de carácter histórico con fines, por ejemplo, de investigación. Evidentemente, este ejercicio de conservación deberá contar con todas las garantías que reconoce la Ley. Lo cierto es que la posibilidad de conservar datos del pasado encuentra un escollo en la redacción de la LOPD. El mandato al responsable del fichero de cumplir con el principio de veracidad tiene en el artículo 4.4 de la LOPD una redacción no demasiado afortunada[1203]. En dicha disposición se establece la obligación del responsable de cancelar de oficio los datos que no cumplan con el requisito de actualidad. Esta disposición podría interpretarse de forma que pudiera ser requerida la cancelación automática de los datos del pasado, y ya se ha dicho que la obligación general de cancelar dichos datos de forma automática podría plantear problemas prácticos en ámbitos como el sanitario.

Se ha de interpretar el artículo de la LOPD que se comenta de tal forma que la cancelación de los datos del pasado no sea un ejercicio automático. Con esta conclusión tampoco se afirma,

[1198] Resoluciones AEPD, R/00977/2006, 18 de enero de 2007, procedimiento TD/00397/2006; R/00857/2006, de 20 de diciembre de 2006, procedimiento TD/00355/2006.
[1199] Resolución AEPD, R/01680/2008, de 27 de noviembre de 2008, procedimiento TD/00473/2008. La línea interpretativa planteada por estos tribunales puede variar en atención a los recursos interpuestos por la agencia.
[1200] RUIZ CARRILLO, *El Tratamiento…,* cit., 2008, pp. 41-42.
[1201] Artículo 4.5 LOPD.
[1202] Artículo 17.1 LBAP.
[1203] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 26.

como parece que se ha pretendido por algún autor[1204], que la conservación de la información del pasado sea la regla general, pues esto podría llevar a que se mantuvieran datos de las personas sin otra finalidad que la de crear perfiles personales más completos. Únicamente se señala que la cancelación no ha de ser automática y que deberá analizarse cada caso para ver si la conservación puede ser necesaria para cumplir con fines legítimos que justifiquen dicho almacenamiento. En todo caso, los supuestos en que se entiende justificado conservar datos concernientes al pasado del titular deberán estar identificados en el ordenamiento. Hay que tener en cuenta, como se ha subrayado, el efecto negativo que este tipo de tratamiento puede conllevar para el derecho a la autodeterminación informativa y otros derechos. No puede ser el responsable del fichero quien decida cuándo puede mantener esta clase de información, sino que deberá ser el propio ordenamiento el que, en beneficio de la seguridad jurídica, concrete estos supuestos.

De lo dicho hasta ahora se concluye que el principio de veracidad reconoce la necesidad de que los datos de carácter personal reflejen, en todo momento, la realidad actual a la que se refieren, si bien, con el matiz de que pueden darse casos en que es necesario conservar datos que reflejan la realidad del pasado para conseguir determinados fines previamente previstos por las leyes.

En segundo lugar, la necesidad de que la actualización se produzca en todo momento podría ser cuestionada si se lleva a cabo un ejercicio comparativo entre diferentes normas. Si se atiende a la redacción de la Directiva[1205] y al Convenio anterior a ésta[1206] puede interpretarse que la exigencia de actualización se limita a determinados momentos. En ambas normas se recoge que la actualización de los datos se dará "cuando sea necesario". De esta expresión podría deducirse que no en todos los casos hace falta actualizar los datos, y que hay circunstancias que hacen que dicha puesta al día no sea necesaria. Si hay supuestos en que la actualización es necesaria habrá otros supuestos en que no lo es.

En relación a los preceptos que se acaban de citar se interpreta que lo que disponen estas normas supranacionales no es que en determinados casos sea necesario actualizar los datos y en otros no. Se entiende que la necesariedad no vendrá de las circunstancias, sino del hecho de que haya datos que no respondan a la realidad actual. Es decir, en las normas europeas la exigencia de actualización deriva del hecho mismo de que haya datos que no han sido puestos al día. No se reconoce la posibilidad de que unos datos no respondan a la realidad actual y se mantengan sin actualizarse porque las circunstancias no lo requieren. Siempre que haya unos datos que no reflejen la realidad presente y, evidentemente, siempre que se conozca que dichos datos pertenecen al pasado, habrá que actualizarlos independientemente de las circunstancias de cada caso. Así se reconoce en la Ley estatal. En la LOPD, no se emplea la expresión "cuando

[1204] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 27.

[1205] Artículo 6.1.d) Directiva 95/46/CE: "*Los estados miembros dispondrán que los datos personales sean: d)exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueros recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados"* (el subrayado es nuestro).

[1206] Artículo 5.d) Convenio 108/ 1981 del Consejo de Europa: "*Los datos de carácter personal que sean objeto de un tratamiento automatizado: d)serán exactos y si fuera necesario puestos al día"* (el subrayado es nuestro).

sea necesario", y así la exigencia de actualización se da, como ha reconocido la propia AEPD, "en todo momento"[1207]. Otra cosa será que también sea necesario mantener datos que reflejan situaciones del pasado para la consecución de la finalidad que justificó la recogida de la información.

IV.1.3. Análisis del contenido del principio de veracidad partiendo del artículo 44.3.f) de la LOPD.

Más allá de lo comentado hasta ahora sobre el requerimiento de que los datos estén actualizados, para comprender de forma adecuada la exigencia que plantea el principio de veracidad hay que realizar un apunte sobre el artículo 44.3.f) de la Ley, que sanciona el incumplimiento de dicho principio[1208].

Es de advertir que se han planteado problemas de interpretación a la hora de decidir qué precepto de la LOPD hay que aplicar para sancionar dicha conducta vulneradora del principio que se analiza, pues en la norma se encuentran diferentes disposiciones que se solapan entre sí[1209]. En el artículo 44.3.f) se recoge expresamente como sancionable el mantener los datos inexactos o no atender a los requerimientos de rectificación o cancelación. Por su parte, en el artículo 44.3.d) se sanciona el manipular datos de carácter personal vulnerando los principios y garantías establecidos en la Ley[1210].

No cabe duda de que el primer precepto, concreto, puede incluirse en el segundo, más genérico. Conviene recordar en este momento que las leyes exigen que la tipificación de infracciones y sanciones administrativas se realice siempre de la manera más clara y precisa posible por las leyes y reglamentos[1211]. Se trata de que los ciudadanos reconozcan de manera inequívoca qué acciones constituyen una infracción[1212]. Si bien es cierto que en la actualidad son innumerables los supuestos en que la indeterminación acompaña a los preceptos que regulan las infracciones y sanciones[1213], no hay que dejar de apuntar que, debido a su ambigüedad, y a falta de un reglamento que desarrolle lo establecido en esta disposición, el citado artículo 44.3.d) de la LOPD no es un modelo a seguir a la hora de tipificar las conductas sancionables[1214]. En este

[1207] Resolución AEPD de 31 de mayo 2007 sobre expediente nº 00224/2005, punto 2.
[1208] Artículo 44.3.f) LOPD: "*Son infracciones graves: Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los drechos de las personas que la presente Ley ampara"*.
[1209] GUERRERO ZAPLANA, "Tipos de infracciones ...", cit., 2008, p. 670.
[1210] Artículo 44.3.d) LOPD: "*Son infracciones graves: Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave"*.
[1211] En la Ley Vasca 2/1998, 20 de febrero, reguladora de la Potestad Sancionadora este requisito se reconoce de manera expresa en el artículo 4: "*Las leyes y normas forales sectoriales configuradotas de los distintos regímenes sancionadores tipificarán las infracciones con la mayor precisión posible (...)*".LASAGABASTER HERRARTE, *Ley de la Potestad...,* cit., 2006, p. 124; SÁNCHEZ MORÓN, *Derecho Administrativo...,* cit., 2007, p. 663; CANO CAMPOS, "Sanciones administrativas…", cit., 2007; GONZÁLEZ TOBARRA y JIMÉNEZ CARBAJO, "El principio de legalidad…", cit., 2009, pp. 139-140.
[1212] SSTC, 8 de junio de 1988, FJ 2 y 11 de febrero de 2002, FJ 4.
[1213] LASAGABASTER HERRARTE, *Ley de la Potestad...,* cit., 2006, p. 127.
[1214] Resolución de la AEPD, R/00520/2009, de 16 de marzo de 2009, procedimiento PS/00546/2008.

último artículo podrían tener cabida muchas actuaciones que aparecen tipificadas en la norma como sancionables. La propia jurisprudencia así lo ha reconocido[1215]. Realmente, como se verá a continuación, la utilidad del precepto es cuestionable e incluso podría plantearse su inconstitucionalidad debido precisamente a su carácter genérico[1216]. En todo caso, como se ve, la vulneración del principio de veracidad puede incluirse tanto en una como en otra disposición. En principio parece coherente que se incluya en el tipo más concreto. No obstante, tanto la jurisprudencia como la AEPD en sus resoluciones han incluido de manera aleatoria en uno u otro artículo dichas actuaciones sancionables.

Centrando el análisis en el precepto más concreto que sanciona la vulneración del principio de veracidad, se puede afirmar que esta disposición reconoce que se vulnerará el principio cuando se mantengan datos que no respondan de forma exacta a la realidad actual o no se hagan efectivos los derechos de cancelación o rectificación ejercidos por el titular de los datos, en los casos en que se vean afectados los derechos del mismo. De una interpretación literal del precepto puede desprenderse que la vulneración del principio de veracidad puede llevarse a cabo a través de dos tipos de actuaciones: mantener datos que no respondan de forma exacta a la realidad actual, o no hacer efectivos los derechos de cancelación o rectificación. No obstante, esta disposición plantea una serie de interrogantes que han dado pie a diferentes interpretaciones de lo que se entiende por vulneración del principio de veracidad.

Una primera interpretación del artículo 44.3.f) ha llevado a pensar que se vulnera el principio, exclusivamente, cuando se niega al titular de los datos de carácter personal el ejercicio de rectificación o cancelación de los datos[1217]. En algún caso la propia jurisprudencia ha parecido seguir esta línea interpretativa[1218]. Se exige para poder encajar una actuación en este tipo que se incluya un dato erróneo en el fichero, el ejercicio por parte del titular de los datos del derecho de rectificación o cancelación y, por último, el mantenimiento por parte del responsable del fichero del dato inexacto a pesar del ejercicio de la rectificación o cancelación por parte del titular[1219]. Según esta línea interpretativa el mero mantenimiento de datos no-veraces en un fichero de datos no sería sancionable en base a este precepto. Esta última conducta sería sancionable siempre que estuviera acompañada, cuando menos, de una falta de diligencia del responsable del fichero, atendiendo a la genérica disposición 44.3.d), como acción que vulnera los principios y garantías recogidas en la LOPD. Así, por un lado, el no hacer efectivos los derechos de cancelación o rectificación se encontraría recogido en el artículo que expresamente sanciona la vulneración del principio de veracidad, y el mero mantenimiento de datos no-veraces en el fichero

[1215] SAN 27 de octubre 2004.
[1216] SAN de 27 octubre 2004, FJ 3.
[1217] Así lo sugería la parte demandante en la SAN de 27 octubre 2007, FJ 3: "la inclusión de datos inexactos en un fichero sólo será conducta sancionable cuando, ejercitados los derechos de rectificación o cancelación, tales derechos fueran denegados por el responsable del fichero".
[1218] STSJ Comunidad de Madrid 10 de mayo del 2000, FJ 3.
[1219] Resolución de la AEPD, R/00301/2006, de 16 de mayo de 2006, procedimiento PS /00149/2005. Punto 2: "La citada sentencia anuló la resolución impugnada, señalando que en dicho supuesto la tipificación adecuada debería haber sido la del artículo 43.3.d) de la LORTAD, actual 44.3.d) de la LOPD, precisamente la misma que se imputa en el presente procedimiento sancionador ya que no ha habido ejercicio de derecho de rectificación de los datos, y, por tanto, no se imputa el hecho de mantener el dato erróneo, sino disponer de datos de la denunciante no exactos y veraces, lo que infringe el principio de calidad de datos".

encontraría acogida en el artículo genérico que sanciona las vulneraciones a los principios y garantías recogidas en la Ley.

Una segunda interpretación, por el contrario, entiende que el artículo 44.3.f) sanciona dos acciones en vez de solamente la que recoge el no hacer efectivos los derechos de rectificación y cancelación: mantener datos de carácter personal inexactos y no efectuar las rectificaciones o cancelaciones de los mismos. Esta interpretación también ha sido seguida en algún caso por la jurisprudencia, que ha llegado a imponer una doble sanción por llevar a cabo las dos acciones citadas, por considerarlas vulneradoras del principio de veracidad[1220].

Un análisis riguroso del principio de veracidad exige llevar a cabo una aclaración. Indudablemente, la falta de ejecución por parte del responsable del fichero de los derechos de rectificación y cancelación conlleva sanción. Pero el "mantener" datos de carácter personal inexactos o incompletos por falta de diligencia del mismo responsable también ha de acarrear sanción administrativa, en base al precepto que recoge la vulneración del principio de veracidad. Este último hecho afecta negativamente al derecho a la autodeterminación informativa. El mero mantener datos no-veraces referidos a una persona identificada o identificable crea un perfil del individuo que no se corresponde con la realidad. Si se entiende que el derecho a la autodeterminación informativa reconoce la facultad de controlar los datos referidos a una persona, en la medida en que esos datos no responden a la realidad, esa facultad de control se ve desde un inicio vulnerada. Las consecuencias que ello conlleva son muy graves. Imagínese si, por ejemplo, alguna entidad tiene acceso a dicho perfil y toma decisiones que afectan al titular de los datos basándose en el mismo. El hecho de que el responsable del fichero tenga datos erróneos debido a su falta de diligencia[1221], independientemente de que se haya ejercido el derecho de rectificación o no, ha de ser sancionado, puesto que esta circunstancia genera una situación de la cual pueden derivar daños para el titular de los datos. Así parecen haberlo entendido recientemente la jurisprudencia[1222] y las resoluciones de la AEPD[1223]. Se reconocen, por tanto, dos acciones diferentes que afectan negativamente al principio de veracidad y que son merecedoras de sanción: mantener los datos erróneos y no ejecutar el derecho de rectificación o cancelación cuando sea requerido[1224].

El precepto que sanciona la vulneración del principio de veracidad plantea una segunda cuestión. Se trata del empleo del término "mantener" para definir la conducta sancionable. Se sanciona la actuación dirigida a mantener datos no-veraces. Este concepto denota cierta temporalidad. Es decir, mantener parece exigir que los datos erróneos tengan que estar cierto tiempo en el fichero para que la conducta sea sancionable. No se habla en la LOPD de "incluir" dichos datos en un fichero. Para que haya sanción será necesario que los datos erróneos estén un intervalo de tiempo en el fichero o soporte correspondiente. Así, podría concluirse que tener

[1220] SAN 19 de noviembre 2003, FJ 5.
[1221] SAN 6 de febrero de 2008; Resolución de la AEPD, R/01513/2008, de 19 de noviembre de 2008, procedimiento AP/00030/2008, apuntan la necesidad de elementos de culpabilidad para poder aplicar el precepto que sanciona la vulneración del principio de veracidad.
[1222] SAN 27 de febrero de 2008.
[1223] Resolución de la AEPD, R/01612/2008, de 3 de diciembre de 2008, procedimiento PS/00419/2008.
[1224] SAN 19 de noviembre 2003, FJ 5.

en un momento determinado datos erróneos no vulnera el principio de veracidad. Así lo han reconocido en alguna ocasión los tribunales[1225].

No se está de acuerdo aquí con esta interpretación. El mero hecho de incluir datos falsos en un fichero, teniendo en cuenta el alcance del principio de veracidad, genera el riesgo de que esos datos puedan ser manipulados. Y ya se ha dicho que la manipulación de datos erróneos puede acarrear consecuencias de gravedad para su titular. Así, se puede entender que el incluir datos erróneos puede ser sancionable, atendiendo al mismo fundamento, si la causa del defecto en el dato es imputable al responsable. Además, el requerimiento de "mantener" puede llevar a pensar que el tipo a sancionar exige que en la actuación del responsable del fichero haya una actitud determinada: saber que los datos son erróneos y a pesar de ello no modificarlos. En algún caso se planteó que la actividad de mantener podía requerir "una voluntad consciente"[1226]. No obstante, de la propia jurisprudencia se puede deducir que no se requiere del factor doloso para vulnerar el principio de veracidad y que basta con la falta de diligencia[1227]. No hace falta una voluntad consciente para que se entienda que el principio de veracidad ha sido vulnerado.

Por otro lado, en la disposición apuntada se señala que el principio de veracidad se vulnerará cuando de este hecho "resulten afectados los derechos de las personas". Parece darse a entender que el contener datos erróneos no constituye por sí solo una actividad sancionable, sino que es necesario que dicha actividad conlleve también la afección a sus derechos. Hay que plantearse si el mero hecho de incluir y mantener datos erróneos no constituye por sí mismo una afección negativa al derecho a la autodeterminación informativa y es, por lo tanto, sancionable.

El derecho a la autodeterminación informativa supone la facultad de controlar los datos de los que uno es titular. En el momento en que el responsable de un fichero incluye información errónea pudiendo haberlo evitado, bien porque el titular ha querido ejercer el derecho de rectificación o cancelación, o bien porque tenía medios para evitar que los datos no respondieran a la realidad actual, se está vulnerando el derecho a la autodeterminación informativa. Si el responsable del fichero incluye datos erróneos, desde la base, el derecho a la autodeterminación informativa aparece vulnerado, pues el derecho a controlar se ejerce sobre un objeto que no se corresponde con la información que se refiere al titular de los datos.

IV.2. El alcance de la obligación de cumplir el principio de veracidad.

IV.2.1. La veracidad en la libertad de información y la imposibilidad de trasladar los criterios que la definen en dicho ámbito al campo de la protección de datos.

Una vez determinado el contenido del principio de veracidad hay que analizar el alcance de la obligación de cumplir dicho principio. Se trata de concretar hasta dónde llega esta obligación.

[1225] STSJ Comunidad de Madrid 10 de mayo del 2000, FJ 3, en la que se entiende que no se vulnera el principio de veracidad por el mero hecho de incluir datos erróneos, si, una vez se tiene constancia de la existencia de dichos errores, se actualizan.
[1226] SAN 12 de mayo 2000, FJ 2, en argumentos presentados por la parte recurrente.
[1227] SAN 12 de mayo 2000, FFJJ 4 y 5.

Para ello, puede resultar de utilidad estudiar, aunque sea brevemente, el tratamiento que se le ha dado al principio que aquí se analiza en otro campo del derecho[1228].

El principio de veracidad ha constituido un punto de análisis importante en el estudio de otro ámbito del derecho como es el de la libertad de comunicar o recibir información, recogida en la Constitución como derecho fundamental[1229]. La veracidad se erige en un elemento de gran relevancia en este ámbito[1230]. No corresponde ahora llevar a cabo una investigación completa sobre los diferentes aspectos de este derecho, pero merece la pena apuntar brevemente lo que el principio de veracidad significa aquí.

Como reconoce la propia Constitución, la libertad de información, distinta a la libertad de expresión[1231] aunque necesariamente relacionada con ésta[1232], tiene como límites, entre otros, la intimidad, el honor y la imagen de las personas sobre las que se informa[1233]. El derecho a la libertad de información no puede ejercerse si vulnera injustificadamente estos otros derechos. No obstante, esta vulneración se considera justificada cuando concurren una serie de elementos en el ejercicio del derecho[1234]. En el caso de la vulneración del derecho al honor en concreto[1235], la limitación de dicho derecho por el ejercicio del derecho a la libertad de información puede entenderse justificada cuando la información cumple con una serie de requisitos, entre otros, que la información sea de interés general y veraz[1236]. Se puede ejercer la libertad de información aunque afecte al honor de un ciudadano, si esa información es de interés general y veraz[1237]. Estos dos requisitos plantean en la práctica muchos matices, que se han puesto de manifiesto en

[1228] GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 80, pone también de manifiesto la importancia de analizar el principio de veracidad en otros ámbitos de la realidad.
[1229] Artículo 20.1.d) CE.
[1230] ROMERO COLOMA, "La Libertad...", cit., 2001, pp. 146-157; ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 356; LAZCANO BROTÓNS, "Comentario al artículo 10…", cit., 2009, p. 481.
[1231] STC 15 de enero de 2007, FJ 4. CARMONA SALGADO, *Libertad de Expresión...*, cit., 1991, pp. 7-8; ORTEGA GUTIÉRREZ, *Derecho a la Información...*, cit., 1999, p. 112; SANJURJO REBOLLO, *Manual de Derecho…,* cit., 2009, p. 70.
[1232] SARAZA JIMENA, *Libertad de Expresión...*, cit., 1995, pp. 163-168.
[1233] Artículo 20.4 CE. ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 413; COUSIDO GONZÁLEZ, "El derecho de la información…", cit., 2007, p. 67.
[1234] ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 417.
[1235] La *exceptio veritatis* no opera en relación al derecho a la intimidad según ha afirmado la doctrina e incluso el TC: SARAZA JIMENA, *Libertad de Expresión...,* cit., 1995, pp. 237-238: p. 238: "mientras en el primer caso (derecho al honor) la veracidad funciona como causa legitimadora de la intromisión, no ocurre lo mismo respecto de la intimidad, en la que juega exclusivamente como causa legitimadora la relevancia pública"; CATALÁ i BAS, *Libertad de Expresión...*, cit., 2001, p. 377: "El TEDH afirma (...) que la exceptio veritatis no ampara, en principio, las informaciones vertidas sobre la vida privada (...). Doctrina plenamente admitida por el Tribunal Constitucional, que en su sentencia 172/1990, de 12 de noviembre (...) afirmará también que el requisito de veracidad entra en juego con relación al derecho al honor pero que, en principio, no despliega sus efectos cuando el derecho que entra en conflicto con la libertad de información es el derecho a la intimidad"; MEDINA GUERRERO, *La Protección...*, cit., 2005, pp. 100-102. STC 12 noviembre de 1990, FJ 3: "El criterio para determinar la legitimidad o ilegitimidad de las intromisiones en la intimidad de las personas no es el de la veracidad, sino exclusivamente el de la relevancia pública del hecho divulgado, es decir, que su comunicación a la opinión pública, aun siendo verdadera, resulte ser necesaria en función del interés público del asunto sobre el que se informa".
[1236] STC 13 de marzo de 2006, FJ 3.
[1237] El requisito de veracidad no opera en el ámbito de la libertad de expresión, pues, como se ha dicho repetidas veces por parte de la doctrina, lo que se protege con este derecho es la facultad de emitir valoraciones y opiniones sobre las que no cabe llevar a cabo el juicio de veracidad: CARMONA SALGADO, *Libertad de Expresión...,* cit., 1991, pp. 174-176; SALVADOR CODERCH y CASTIÑEIRA PALOU, *Prevenir y castigar...*, cit., 1997, pp. 60-61; ORTEGA GUTIÉRREZ, *Derecho a la Información...*, cit., 1999, pp. 120-122.

gran medida en las decisiones tomadas por el TEDH al tratar la libertad de información[1238]. Basta aquí con señalar las características fundamentales que han de guardar.

La información será de interés general cuando afecte a una persona con relevancia pública o cuando los hechos que se relatan, en sí mismos, pueden ser considerados como noticiables para la opinión pública[1239]. En cuanto a la veracidad, este requisito en el ámbito de la libertad de información no se refiere a que, en todo caso, la información que se emite sea verdadera y refleje con exactitud la verdad objetiva o histórica[1240]. Lo que se exige en este ámbito es que quien emite la información haya actuado con la suficiente diligencia como para contrastar, en base al nivel de exigencia que establecen en este momento los cánones de profesionalidad atendiendo a cada caso[1241], la veracidad de dicha información, independientemente de que luego sea completamente cierta o no[1242], de tal forma que no queda lugar para los meros rumores o invenciones sin contrastar[1243]. Lo realmente importante es que el responsable de que la información se emita haya hecho todo lo posible por cerciorarse de la veracidad de la información[1244], sin que este deber de diligencia requiera esfuerzos desproporcionados por parte del informador[1245].

Este esquema de análisis de la veracidad no es válido para el estudio del principio de veracidad en el ámbito que aquí se trata. Es evidente que el derecho a la libertad de la información y el derecho a la autodeterminación informativa, si bien pudieran estar relacionados en algunos aspectos, se refieren a realidades distintas con sus propias particularidades. Más allá de que cada derecho abraza distintas facultades, hay que tener en cuenta que en la mayoría de los casos la información a la que se refieren uno y otro derecho tiene ciertas diferencias.

En el derecho a la libertad de la información los datos que se transmiten o reciben pretenden reflejar de forma objetiva la realidad a la que se refieren. No obstante, la mayoría de las veces esa información responde en la práctica a una visión subjetiva o parcial de dicha realidad. Más allá de las dificultades que presenta la distinción entre dato y opinión[1246], en muchas ocasiones, en el ejercicio del derecho a la libertad de la información los datos que se consideran objetivos

[1238] LAZCANO BROTÓNS, "Comentario al artículo 10…", cit., 2009, p. 452.
[1239] STC 4 de junio de 2007, FJ 8. ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 360.
[1240] STC 30 de junio de 1998, FJ 4. URÍA, *Lecciones de Derecho…,* cit., 2003, p. 99; ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 356; GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* cit., 2007, p. 252.
[1241] ATC 18 de enero de 2006 FJ 4: "La diligencia exigible a un profesional de la información no puede precisarse *a priori* y con carácter general, pues depende de las características concretas de la comunicación de que se trate, por lo que su apreciación dependerá de las circunstancias de cada caso". CARMONA SALGADO, *Libertad de expresión...*, cit., 1991, pp. 167-172; ORTEGA GUTIÉRREZ, *Derecho a la Información...*, cit., 1999, pp. 124-125; URÍA, *Lecciones de Derecho…,* cit., 2003, p. 101; SÁNCHEZ FERRIZ, *Delimitación de las libertades...*, cit., 2004, pp. 166-168; GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* cit., 2007, p. 258.
[1242] SSTC 25 de febrero de 2002, FJ 6 y 3 de julio de 2006, FJ 5. CARRILLO, "Derecho a la información…", cit., 1988, p. 204; CARMONA SALGADO, *Libertad de Expresión...*, cit., 1991, p. 165; SARAZA JIMENA, *Libertad de Expresión...*, cit., 1995, p. 240; BARATA i MIR, "Veracidad y Objetividad…", cit., 2003, p. 317; SANJURJO REBOLLO, *Manual de Derecho…,* cit., 2009, p. 67
[1243] GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* cit., 2007, pp. 253-254.
[1244] SALVADOR CODERCH y CASTIÑEIRA PALOU, *Prevenir y Castigar...,* cit., 1997, p. 19-53; ROMERO COLOMA, *Libertad de Información…,* cit., 2000, p. 50.
[1245] CARMONA SALGADO, *Libertad de Expresión...*, cit., 1991, p. 167-168.
[1246] MUÑOZ LLORENTE, *Libertad de Información…*, cit., 1999, p. 88.

aparecen mezclados con valoraciones y opiniones subjetivas[1247]. No hay más que ver como un mismo hecho puede ser interpretado y narrado de formas tan diferentes por un medio de comunicación u otro.

Por el contrario, en el caso del derecho a la autodeterminación informativa, en la mayoría de los casos la información que se recoge en los ficheros son datos objetivos que reflejan con escrupuloso rigor la realidad, y nada más que eso, de las personas a las que se refieren los datos. En general los ficheros recogen datos que reflejan estrictamente la realidad de las personas a las que se refieren: nombre y apellidos, dirección, trabajo, estatura, afiliación sindical, etc. Hay que apuntar, sin embargo, que en ocasiones esta información objetiva se ve acompañada de valoraciones subjetivas sobre los titulares de los datos. En el ámbito de la sanidad, por ejemplo, los datos objetivos del paciente aparecen junto a valoraciones subjetivas de los profesionales sobre el sujeto y sus afecciones: posibles diagnósticos, interpretaciones de las dolencias, etc. Lo mismo ocurre en los ficheros en que se pretenden crear perfiles sobre los gustos y preferencias de determinados sujetos partiendo de datos objetivos sobre los mismos. En todo caso, parece clara la diferencia entre el tipo de información que se manipula en general en las dos disciplinas citadas, la protección de datos y la libertad de información.

Esta distinción resulta importante por cuanto que marcará el diferente alcance de la responsabilidad a exigir a quien manipula la información en uno y otro ámbito. Evidentemente, en relación al derecho a la autodeterminación informativa, al estar manipulando información exacta, objetiva, se requerirá al responsable que conserve los datos de manera que reflejen la realidad exacta del titular de los mismos, cosa que no ocurre cuando se trata del ejercicio de la libertad de información.

Atendiendo a la realidad que abrazan cada uno de los derechos parece lógico afirmar que el principio de veracidad no cumple el mismo papel en uno u otro ámbito. Precisamente, la principal diferencia entre los dos ámbitos con respecto a la forma de tratar la información se presenta, no en el tipo de información que se trata, sino en los efectos que produce el incumplimiento del principio de veracidad en uno u otro sector. En relación al derecho a la libertad de la información la falta de veracidad afectará fundamentalmente al honor, la intimidad o la imagen de las personas a las que se refiere la información. En este ámbito, probablemente uno de los mayores problemas que surgen, debido a la utilización de información no veraz, es la generación de "rumores"[1248], la mala información, lo cual, más allá de afectar a la intimidad, honor o propia imagen de una persona individual, genera una visión falsa de la realidad en el público en general.

Por el contrario, en el ámbito de la protección de datos de carácter personal las consecuencias son otras. Ya se ha dicho que la manipulación de datos de carácter personal constituye un medio para alcanzar un fin concreto. Los fines que se persiguen con el tratamiento de esta información son muy variados. En muchos supuestos las finalidades tienen que ver con materias especialmente relevantes, como pueden ser la seguridad nacional, la prevención de delitos o la protección de la salud de las personas. En estos casos el empleo de datos erróneos

[1247] CARRILLO, "Derecho a la información…", cit., 1988, p. 190.
[1248] STC, 13 de marzo de 2006, FJ 3. SÁNCHEZ FERRIZ, *El Derecho...*, cit., 1974, p. 70.

acarrea graves consecuencias[1249]. Evidentemente, el uso de datos inexactos conlleva la toma de decisiones erróneas, lo cual supone que el fin perseguido no se alcance, no por lo menos de manera satisfactoria. Las consecuencias de manipular información errónea en este ámbito pueden ser mucho más graves que las que puedan darse en el ámbito de la libertad de información en forma de afección al honor, la intimidad o la imagen. En el ámbito sanitario el trabajar con información no ajustada a la realidad actual del paciente puede tener resultados nefastos; dar un tratamiento equivocado a un paciente puede ser fatal. En estos supuestos la consecuencia de manipular información errónea no sólo es una posible vulneración del derecho a la autodeterminación informativa, sino la afección de manera negativa en la salud de las personas.

IV.2.2. El alcance del principio de veracidad en el ámbito de la protección de datos.

Teniendo en cuenta las diferentes consecuencias que puede tener el emplear información no-veraz en los ámbitos citados, parece evidente que las exigencias que derivan del principio de veracidad tendrán un alcance diferente en dichas disciplinas. En el ámbito de la protección de datos la diligencia de quien manipula la información habrá de ser mayor por las consecuencias que puede acarrear la vulneración de dicho principio. La veracidad exige aquí que los datos sean exactos en todo momento, mientras que cuando se refiere al ejercicio de la libertad de información se limita a requerir una actividad diligente del informador, independientemente de que los datos remitidos no sean exactos ni se correspondan con la realidad. La obligación del responsable del fichero no será simplemente de contrastar la información, como ocurre con el principio de veracidad en el derecho fundamental a la libertad de información, sino de mantener los datos en todo momento de tal forma que reflejen la realidad actual del titular de los datos[1250].

Como ha dispuesto la LOPD, el cumplimiento del principio de veracidad en el ámbito de la protección de datos de carácter personal requiere de un sistema de medidas dirigido a garantizar, que la información que se trata en cualquier situación refleje, desde el momento de la recogida hasta que se suprimen, con exactitud y actualidad, toda la realidad a la que se refieren. Se puede hablar de la instauración en la Ley de una serie de obligaciones para el responsable del fichero y una serie de derechos para el titular de los datos de carácter personal, como medidas dirigidas a la salvaguarda del principio de veracidad. En lo que corresponde al responsable del fichero, la obligación de hacer todo lo posible por mantener la veracidad de los datos queda claramente reflejada en la Ley: "*si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16*"[1251]. En esta misma línea, tras asumir este criterio general aportado por la Ley, el RDLOPD apuntaba una alternativa concreta dirigida también a asegurar la veracidad de los datos a tratar en el ámbito de la Administración electrónica. Señalaba esta disposición general que los órganos administrativos podrán verificar la autenticidad de los datos que les lleguen en

[1249] ARENAS RAMIRO, *El Derecho...*, cit., 2006, p. 320; SANZ CALVO, "Calidad de los datos…", cit., 2008, p.155.
[1250] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 187.
[1251] Artículo 4.4 LOPD.

solicitudes tramitadas por vía electrónica en las que se incluya información[1252]. Los tribunales han anulado este precepto, al entender que permite un tratamiento sin consentimiento del titular, carente de justificación[1253]. Si bien esta decisión plantea alguna duda de interpretación y no se basa en un análisis especialmente riguroso, hay que subrayar, aunque sea a modo de testimonio, que aporta ciertas garantías en el tratamiento de datos por parte de la Administración, al someter a una habilitación legal específica la posibilidad de que los órganos administrativos manipulen información con el fin de verificar la autenticidad de determinados datos.

Centrado el estudio en la letra de la LOPD, lo cierto es que la Ley no establece un criterio definido sobre el alcance de las obligaciones del responsable del fichero en el cumplimiento del principio de veracidad[1254]. El análisis de este principio en el ámbito de la protección de datos se ha llevado a cabo fundamentalmente por la jurisprudencia en el estudio de los ficheros de solvencia patrimonial. Es de este análisis de donde se han de sacar conclusiones. Este tipo de ficheros plantea numerosos interrogantes[1255].

En la mayoría de supuestos vinculados a estos ficheros los ciudadanos aparecen por error como morosos. Las consecuencias de este hecho pueden ser varias, pero en la práctica, la mayoría de casos se relacionan con la denegación de créditos[1256] y la generación de dificultades en el desarrollo de actividades financieras[1257]. En los casos referidos a la información sobre solvencia patrimonial se reconocen dos ficheros: el del acreedor, que manipula los datos de una persona que le debe dinero, y el fichero común en el que se recogen los datos de diferentes personas que aparecen como morosas y al que acceden generalmente diferentes entidades para conocer la solvencia de posibles clientes. Los acreedores remiten al fichero común los datos sobre el cliente moroso, de tal forma que en ese segundo fichero se acumulan los datos de las personas que en principio deben dinero a diferentes entidades. Pues bien, partiendo de ese flujo de información se plantea la jurisprudencia una cuestión: ¿debe el responsable del segundo fichero asegurarse de la veracidad de los datos que se le comunican? Del análisis que la jurisprudencia ha llevado a cabo sobre esta cuestión se ha de intentar extraer conclusiones que aporten luz sobre el alcance de la obligación del responsable del fichero de cumplir con el principio de veracidad.

En primer lugar, se puede concluir que el principio de veracidad no conduce a una responsabilidad objetiva. Para que la vulneración de este principio conlleve cierta responsabilidad es necesario que el error sea imputable de alguna forma a una acción u omisión del responsable del fichero que refleje, cuando menos, una falta de diligencia por su parte. Es decir, si el

[1252] Artículo 11 RDLOPD: "*Cuando se formulen solicitudes por medios electrónicos en las que el interesado declare datos personales que obren en poder de las Administraciones públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la autenticidad de los datos*".
[1253] STS 15 de julio de 2010, FJ 6.
[1254] APARICIO SALOM, "La Calidad…", cit., 2010, p. 331, se plantea, por ejemplo, si esta obligación de actualizar de oficio alcanza a exigir al responsable del fichero una investigación de los hechos a los que se refieren los datos, para determinar si la información se adecua a la realidad.
[1255] GRACIANO REGALADO, "Ficheros de Información...", cit., 2005, p. 1.722.
[1256] SAN 18 de julio 2007, FJ 4; SANZ CALVO, "Calidad de los datos…", cit., 2008, p. 155.
[1257] SAN 22 de diciembre 2000, FJ 3; SAN 19 de enero 2001, FJ 1.

responsable no tiene forma razonable alguna de evitar el error en los datos no puede erigirse en infractor. En la jurisprudencia que ha analizado las características de los ficheros de solvencia patrimonial, se imputa al acreedor la vulneración del principio de veracidad cuando por su falta de diligencia mantiene y manipula datos erróneos o incompletos[1258].

En segundo lugar, hay que tratar de determinar el nivel de responsabilidad que cabe atribuir a cada sujeto que participa en el tratamiento de datos en el cumplimiento del principio de veracidad. La responsabilidad variará según el supuesto. En algunos casos, la información la recoge el responsable del fichero del titular de los datos. Si es el propio titular quien transmite dichos datos de forma errónea, es obvio que no puede imputársele responsabilidad alguna al responsable del fichero por incumplimiento del principio de veracidad. Como señala el reglamento de desarrollo de la LOPD, se parte de la consideración de que los datos remitidos por el propio titular son exactos[1259]. No se puede exigir al responsable que, de oficio, verifique la exactitud de los datos aportados por el propio titular[1260].

Cuando el responsable del fichero recaba la información del propio titular, puede entenderse que el primero vulnera el principio de veracidad en diferentes circunstancias. Primero, cuando el titular ejerce el derecho de rectificación o cancelación y el responsable del fichero no hace efectivo el mismo. Y segundo, cuando en el momento de manipular los datos recogidos directamente por el titular, se produzca un error imputable al responsable y los recoja o manipule de manera incorrecta y sin que reflejen la realidad actual. En estos casos, aunque sean pequeños fallos informáticos, según la jurisprudencia ya citada, la falta de diligencia también es sancionable. También podrá considerarse como responsable de vulnerar el principio de veracidad cuando de los datos que le ha otorgado el titular genera nueva información, que no es acorde con la realidad actual del titular.

Cuando los datos han sido recabados de fuente distinta al titular la situación es otra. Esta circunstancia puede darse en el caso de la cesión de datos y en el supuesto en que la información es recogida de fuentes accesibles al público. En estas situaciones es más probable que pueda haber errores y que dichos datos sean empleados de forma inadecuada pues son más los agentes que entran a manipular la información. El error puede venir tanto de quien transmite los datos como del que los recoge.

En el caso de la cesión habría que ver si el cedente ha recogido los datos con los correspondientes errores, es decir, si los errores se han producido en la transmisión de los datos por parte de su titular al que va a ser el cedente, o si los errores se deben a la falta de diligencia de este último a la hora de recoger los datos de su titular. En este último caso la responsabilidad es del cedente, sin embargo, en el primer supuesto no se le puede imputar responsabilidad alguna. El cedente puede cometer algún error también a la hora de transmitir los datos al cesionario. En esta situación la vulneración del principio de veracidad le será también imputada. En los casos de los ficheros de solvencia patrimonial, cuando el responsable del primer fichero

[1258] SAN 15 de diciembre 2005, FJ 5.
[1259] Artículo 8.5 RDLOPD: "(…) *Si los datos fueran recoditos directamente del afectado, se considerarán exactos los facilitados por éste*".
[1260] ALMUZARA ALMAIDA, "Relaciones Precontractuales…", cit., 2007, p. 158.

comunica al responsable del segundo fichero datos erróneos el primero será el responsable de vulnerar el principio de veracidad[1261], siempre y cuando hubiera tenido conocimiento de que los datos son erróneos, o dicha circunstancia surja de su falta de diligencia. En todo caso, el responsable del fichero cedente estará obligado a informar de cualquier rectificación o cancelación, de cualquier actualización, que se hubiera producido en los datos que le ha transmitido al cesionario[1262]. El cesionario, por su parte, puede ser también el responsable de la vulneración cuando altera la información, bien porque en la recogida la cambia o porque la almacena de forma que los datos no responden a la verdad. En el caso de la recogida de los datos de fuentes accesibles al público[1263], el error puede estar también en el dato que se recoge, o en su tratamiento por el responsable que recoge dichos datos.

En tercer lugar, ¿hasta dónde ha de llegar la diligencia del responsable del fichero? [1264] De la jurisprudencia y la normativa puede deducirse que no puede exigírsele una diligencia sin límites, sino que tiene que reducirse a un esfuerzo razonable. En este sentido parecen chocar la LOPD y la Directiva. La primera señala que los datos que incumplen con el principio de veracidad serán cambiados "*de oficio*" por los datos adecuados. En cambio, la Directiva europea dispone que *"deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados"*[1265]. Llama la atención, de la lectura de la norma europea, el empleo del adjetivo "razonable"[1266], pues éste no es utilizado por la norma estatal. Esta situación podría llevar a entender que en el ámbito estatal puede exigirse un esfuerzo desproporcionado en la actualización de los datos[1267]. Más allá de que esa interpretación de la Ley atentaría contra lo que dicta la norma europea, carece de sentido alguno el que se le pueda exigir al responsable de los datos una diligencia desmedida en el respeto al principio de veracidad. Necesariamente, este nivel de diligencia a requerir dependerá de cada caso, sobre todo, de las características de

[1261] SAN 13 de julio 2007, FJ. 3. Con la anterior Ley orgánica de protección de datos, no se castigaba a quien cedía los datos de carácter personal, el acreedor, al fichero común, por entenderse que no era responsable de dicho fichero. Esta situación ha variado por completo, y quien remite al fichero común la información errónea se convierte, atendiendo a la actual LOPD, en sujeto vulnerador del principio de veracidad. En el Reglamento que desarrolla la LOPD se zanja este debate, en el artículo 43: "*1. El acreedor o quien actúa por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 35 y 36 en el momento de notificar los datos adversos al responsable del fichero común.*
2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre".

[1262] Artículo 8.5 RDLOPD: "*Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido*".

[1263] Artículo 3.j) LOPD: "*Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes accesibles al público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación"*.

[1264] APARICIO SALOM, *Estudio sobre la Ley*..., cit., 2000, p. 98.

[1265] Artículo 6.1.d) Directiva 95/46/CE.

[1266] GUERRERO PICÓ, *El Impacto*..., cit., 2006, p. 245.

[1267] GARCÍA MESEGUER y MEDRÁN VIOQUE, "España: la Protección...", cit., 2002.

la actividad del responsable del fichero, de la finalidad que se persiga con el tratamiento de los datos y de los bienes jurídicos afectados por dicho tratamiento. La diligencia que se exigirá, por ejemplo, a las Fuerzas y Cuerpos de Seguridad, al periodista o al profesional sanitario en el ejercicio de su actividad profesional, será mayor que la que se solicite a otros agentes. La razonabilidad a la que hace referencia la Directiva europea habrá que entenderla dependiendo del caso concreto. El nivel de diligencia a exigir, por lo tanto, será diferente según el supuesto.

Lo cierto es que si se tiene en cuenta la importancia que tienen algunos datos en la toma de decisiones y el efecto de dichas decisiones sobre las personas, podría pensarse que es exigible un alto índice de diligencia al responsable del fichero, que llegase incluso a exigirle la comprobación de la veracidad de los datos que recoge antes de manipularlos[1268]. Esta idea podría desprenderse también de cierta jurisprudencia que señala que el responsable del fichero ha de hacer todo lo posible por verificar si los datos que maneja son veraces o no[1269]. Si se obliga al responsable del fichero a comprobar en todo caso, de oficio, la veracidad de los datos que tiene en su poder es evidente que se ganará un plus de garantía en la protección del derecho a la autodeterminación informativa, pues habrá una mayor probabilidad de que los datos reflejen la realidad actual a la que se refieren.

La exigencia, sin embargo, de un alto nivel de diligencia plantea problemas desde el punto de vista práctico. El tener que comprobar la veracidad de todos los datos que se reciben podría suponer un coste de tiempo y medios excesivo para el responsable del fichero, que en la mayoría de los casos, obstaculizaría y retrasaría su tarea[1270]. Imagínese que se remiten de un centro sanitario unos datos relativos a la salud de determinadas personas para llevar a cabo un estudio epidemiológico. Podría pensarse que el organismo receptor de los datos está obligado a comprobar la veracidad de los datos recibidos. Esta acción garantizaría, *a priori,* un mayor respeto del principio de veracidad. No obstante, no se puede escapar la idea de que dicha obligación conllevaría también un obstáculo para llevar a cabo la labor de investigación. En el ámbito sanitario se evidencia perfectamente, que la exigencia al responsable de los ficheros de que verifique de oficio la adecuación de los datos que tiene en su poder con la realidad actual, obstaculizaría la labor sanitaria hasta el punto de que en casos, por ejemplo, de urgencia pondría en riesgo algo más que el derecho a la autodeterminación informativa.

Como regla general, por lo tanto, no cabe pedir al responsable del fichero que certifique la veracidad de los datos que recoge. El incluir esta obligación dentro del contenido del principio de veracidad supondría que el responsable vulneraría dicho principio en caso de que no llevase a cabo esta labor de investigación, de oficio, cada vez que recogiese datos de carácter personal. No parece que responda a la lógica el que al responsable del fichero se le sancione por no haber ejercido esa labor de investigador previa.

[1268] VELÁZQUEZ BAUTISTA, *Protección Jurídica...*, cit., 1993, p. 127: "La actualización de la información es una de las obligaciones del creador o gestor de la base de datos, forma parte de su trabajo, se halla conforme se ha indicado directamente relacionada con la calidad del fichero, deberá cumplirse <<de oficio>>. Aunque esto no es óbice para que la actualización de los datos se plantee a partir del ejercicio del Derecho de acceso".
[1269] SAN 13 de junio 2007, FJ 3: "el acreedor sólo puede utilizar tales mecanismos excepcionales que la LOPD le otorga, cuando tenga plena seguridad y certeza de la existencia y cuantía del crédito".
[1270] GUERRERÓ PICÓ, *El Impacto...*, cit., 2006, pp. 245-246.

Esto no quiere decir que en determinadas situaciones el nivel de diligencia a exigir al responsable no sea alto. Hay que tener en cuenta que no todas las situaciones son idénticas y que se pueden encontrar casos en que el nivel de exigencia sea mayor que en otros supuestos. Habrá que atender por lo tanto al caso concreto en el que se tratan los datos, especialmente a los medios que posee el responsable del fichero para verificar si los datos se ajustan a la realidad actual y a la finalidad que se persigue con el tratamiento de los datos[1271].

En este sentido, parece razonable afirmar que en supuestos en que el responsable tiene un mayor interés en el tratamiento de datos para llevar a cabo unos servicios que le reportarán beneficios, la diligencia de dicho responsable deberá ser mayor. Corresponderá al responsable de los datos una mayor carga a la hora de mantenerlos actualizados[1272]. Se está pensando, por ejemplo, en entidades dedicadas a la publicidad, que recogen datos de las fuentes accesibles al público[1273], o en ficheros que se emplean para conocer cuál es la situación económica de los ciudadanos con el fin de prestarles o no un determinado servicio en base a dicha situación[1274].

La exigencia de mayor diligencia puede deberse también a otros motivos. Cuando es la Administración la que manipula la información, la defensa del interés general hace muchas veces que se obligue a los ciudadanos a realizar la tarea de actualización de los datos que se emplean para la consecución de una finalidad de interés común[1275]. La entidad de los bienes jurídicos a proteger puede justificar que se imponga al titular de los datos esta carga. Es lo que ocurre en el ámbito tributario. En otras ocasiones, la carga se le impone a la propia Administración. Es el caso de la actualización del Padrón. La LBRL ha recogido en este caso la necesidad de que la Administración lleve a cabo las actuaciones necesarias para que la actualización de los datos sobre los ciudadanos sea efectiva[1276]. Hay que tener en cuenta que la Administración dispone de numerosos ficheros en los que se recogen multitud de datos sobre los ciudadanos. Se trata de ficheros en los que se puede contrastar la información recogida por última vez por el aparato público. Por lo tanto, la Administración, teniendo medios para hacerlo, tratándose de supuestos en que se defiende un interés general de envergadura deberá actuar con un mayor nivel de diligencia.

Se concluye, por lo tanto, que el nivel de responsabilidad a exigir al responsable de un fichero en el cumplimiento del principio de veracidad variará según el caso concreto ante el que se esté,

[1271] GUERRERÓ PICÓ, *El Impacto...,* cit., 2006, pp. 245-247.
[1272] Resolución de la AEPD, R/00398/2006, 15 de junio de 2006, procedimiento AAPP/00030/2005; SAN 31 de enero de 2003.
[1273] STSJ Comunidad de Madrid de 15 de diciembre del 2000, partiendo de la teoría que hemos expuesto, exige a Caja Rural de Granada que actualice de oficio sus ficheros de morosos, independientemente del esfuerzo que ello le pueda conllevar.
[1274] Resolución de la AEPD, R/01612/2008 , 3 de diciembre de 2008, procedimiento PS/00419/2008.
[1275] GUICHOT, *Datos Personales...*, cit., 2005, p. 228, pone una serie de ejemplos en los que se obliga al titular de los datos, al ciudadano, a comunicar a la Administración los cambios en cierta información concerniente a su persona: cambio de residencia, errores en los datos sobre su patrimonio etc.
[1276] Artículo 17.2 LBRL: "*Los Ayuntamientos realizarán las actuaciones y operaciones necesarias para mantener actualizados sus Padrones de modo que los datos contenidos en éstos concuerden con la realidad*".

pues el grado de diligencia a requerir será diferente dependiendo de los factores que se han analizado[1277].

Lo realmente importante en relación a las garantías que prevé el principio de veracidad no es, sin embargo, el sistema de responsabilidades que se articula. Se entiende aquí que lo fundamental para el escrupuloso respeto de este principio es la fijación por la Ley de medios para que se vea cumplido desde un inicio. Se trata de que se establezcan los instrumentos necesarios para que la información no se altere y, si se altera, pueda restablecerse.

En esta línea la LOPD dispone un sistema de facultades a favor del titular de los datos y de obligaciones que el responsable del fichero ha de cumplir, a través del cual se previene de la producción de errores en los datos que se manipulan y, en caso de producirse, se subsanan antes de que produzcan efectos negativos. El sistema sancionador sólo entra en juego cuando los mecanismos preventivos fallan.

En este sentido, el derecho del titular de los datos a rectificar o/y cancelar los datos inveraces constituye un instrumento indispensable para el correcto cumplimiento del principio. Se trata de facultades que posibilitan que los datos se mantengan exactos, actuales y completos. Sin embargo, en la citada acción preventiva a favor de la protección del principio de veracidad sobresale el derecho a la información, pues permite al titular de los datos desarrollar acciones que hacen posible que el error en el tratamiento sea el mínimo[1278]. Cuando los datos son recabados del propio titular de carácter personal, como es obvio, éste tiene conocimiento inmediato del hecho de que sus datos van a ser manipulados para el cumplimiento de un fin determinado. Lo realmente importante en esta situación, a efectos de que se cumpla el principio de veracidad, es que al titular de los datos se le informe sobre la posibilidad de ejercer los derechos de acceso, rectificación y cancelación y se le facilite el ejercicio de los mismos. En caso de que los datos lleguen al responsable del fichero por un tercero, el titular no tiene conocimiento directo de la cesión. Así, en esta circunstancia, es especialmente relevante que se le informe de ese hecho para que pueda, a través del ejercicio del derecho de acceso, ver si los datos que se van a manipular son ciertos o no. En ambos casos, el derecho a la información constituye la piedra angular para que el cumplimiento del principio de veracidad pueda llevarse a cabo con total garantía, pues supone el primer paso para que el titular de los datos ejerza las acciones oportunas para conocer el contenido de los datos que se refieren a su persona.

IV.3. El principio de veracidad en el ámbito sanitario.

Como se ha visto en las líneas que preceden a este apartado, el principio de veracidad exige que los datos que se vayan a manipular para la consecución de un fin sean, en todo momento, actuales, exactos y completos. Se requiere que la información se corresponda con la realidad presente, que refleje fielmente dicha realidad y que recoja todas las partes o aspectos que

[1277] APARICIO SALOM, "La calidad…", cit., 2010, p. 331, distingue entre los supuestos en que los datos han sido recabados con el consentimiento del titular de los que no. En el primer caso, la participación del titular de los datos lleva a que se pueda solicitar a éste una mayor participación en la actualización de los datos. En el segundo caso, por el contrario, será el responsable del fichero quien deba asumir mayoritariamente este deber de actualizar.
[1278] MARCHENA GÓMEZ, "Conocimiento por el interesado...", cit., 1999, pp. 1-5.

configuran la misma. Se ha puesto de manifiesto también la especial importancia que este requisito guarda en el ámbito sanitario[1279]. Piénsese que la mínima alteración en los datos médicos de un sujeto puede acarrear consecuencias nefastas para su salud u otros derechos o intereses[1280]. Es por ello por lo que en este ámbito el cumplimiento estricto de este principio alcanza su máxima expresión, exigiéndose a los órganos responsables de los diferentes ficheros un alto grado de diligencia. La necesidad de que los datos representen con total objetividad la realidad, sin que haya errores, datos desfasados o incompletos, es en este ámbito especialmente subrayable. En este sentido, la LBAP exige que la información que se maneje en el sector sanitario sea siempre veraz y actualizada[1281].

La responsabilidad de que se cumpla con este principio es, evidentemente, tanto de la Administración sanitaria como de los propios usuarios. Estos últimos, conscientes de la relevancia de transmitir la información más completa y exacta posible deberán ir actualizando los datos referentes a su salud. Los diferentes órganos que configuran la Administración, por su parte, tendrán una doble responsabilidad. Por un lado deberán ser diligentes a la hora de incorporar a los ficheros los datos que ellos mismos recaban o crean, bien directamente de la realización de intervenciones corporales, exploraciones u otras operaciones o bien de interpretaciones que llevan a cabo de la información transmitida por los pacientes. Por otro, deberán guardar el máximo cuidado cuando manipulen los datos de los que disponen.

Hay que tener en cuenta que en este sector se maneja una cantidad ingente de información. Ya se ha apuntado que en las historias clínicas no sólo se refleja la situación actual de la salud de las personas, sino que se da una perspectiva histórica de la misma, conservando datos reales pero no actuales. Este hecho hace que sea más complicado en este ámbito cumplir con los parámetros marcados por la LOPD y en concreto con el principio de veracidad. La necesidad de que los datos que se vayan a emplear para proteger la salud de los ciudadanos cuenten con una "calidad" máxima, ha llevado a que en los sistemas sanitarios se de una importancia de primer orden a los sistemas de información a utilizar en los mismos. Precisamente, los diferentes proyectos de creación de la historia clínica única tienen como justificación principal la necesidad de que desaparezcan islas de información o informaciones duplicadas, que favorecen situaciones en que los errores pueden resultar más fáciles de producirse[1282]. No es lo mismo mantener la veracidad sobre un documento referido a un paciente o sobre una multitud de documentos sobre esa misma persona.

Más allá de estos apuntes la aplicación del principio de veracidad al ámbito estrictamente sanitario no plantea mayores problemas que los que se han señalado hasta ahora en términos generales. No obstante, dadas las especificidades que presenta la práctica sanitaria y, en

[1279] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 140.
[1280] Resolución APDCM, 23 de septiembre de 2009, "El no mantener exactos y puestos al día los datos identificativos de dos pacientes ha supuesto la comisión de una infracción por un hospital de la Comunidad de Madrid", en la que el error en la identidad de un expediente sanitario, al trasladar un parte a la policía, lleva a una persona a ser objeto de investigación policial por error.
[1281] Artículo 15.1 LBAP.
[1282] Artículo 15.4 LBAP: "*La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial*".

especial, la relación entre profesional sanitario y paciente, hay que hacer una serie de consideraciones sobre la aplicación de este principio en este ámbito.

A) Hay que tener en cuenta que el ámbito de la sanidad es un espacio de colaboración entre profesionales y pacientes. Se ha subrayado que la relación que vincula a los profesionales de la sanidad y los pacientes es una relación de confianza. No puede ser de otra manera teniendo en cuenta el fin que se persigue. Los datos que completan los ficheros en el ámbito sanitario surgen de esa relación de confianza, tanto la información que se empleará en la asistencia sanitaria directa como la que se empleará para desarrollar otras actividades como investigaciones, etc. Este hecho hará que la producción de errores en este ámbito sea menor. Necesariamente, en una relación en la que el contacto entre el responsable del fichero y el titular de los datos es más constante, la probabilidad de que se produzcan errores es menor que en otros supuestos.

En todo caso, no es imposible, ni mucho menos, que estos errores se den. Se ha reconocido en las resoluciones de la AEPD algún supuesto de error en la historia clínica de un paciente[1283]. Las alteraciones en la información sanitaria pueden darse sobre los datos meramente objetivos o sobre las interpretaciones que los profesionales sanitarios realizan de dichos datos.

En relación a las interpretaciones hay que realizar un apunte. Hay que tener presente que, en gran parte, la información contenida en los ficheros que se recogen en el ámbito sanitario se trata de interpretaciones que sobre unos datos objetivos llevan a cabo los profesionales. Los datos que dan los pacientes, los que derivan de pruebas que realizan los propios profesionales sanitarios y los que transmiten terceras personas, normalmente parientes o personas cercanas al titular de los datos, son interpretados por los profesionales para extraer conclusiones sobre el estado de la salud del paciente y determinar un diagnóstico. Evidentemente, estas interpretaciones constituyen información sobre los pacientes y pueden no corresponderse con la realidad, pueden ser equívocas. No obstante, el principio de veracidad no se refiere a esta circunstancia.

No afecta a este principio el que un profesional pueda equivocarse interpretando unos hechos de manera errónea e incluyendo así en una historia clínica información que no se corresponde con la realidad actual del titular de los datos. Este hecho hay que relacionarlo con la responsabilidad en la deficiente actividad profesional del médico atendiendo al estado del conocimiento en este ámbito. En este caso se estaría ante una falta de diligencia del profesional, no obstante, esta falta de diligencia, más que en relación a la manipulación de los datos, se produce en relación al ejercicio de su profesión. El margen de error en estos casos es el que se le atribuye al nivel de conocimiento exigible en este momento a la ciencia médica.

Otra cosa es que se descubra que la interpretación que se ha llevado a cabo por un profesional no es adecuada o acorde a la realidad y, a sabiendas de este hecho, se mantenga esa interpretación en la historia clínica como hecho cierto y veraz. En este caso se estará vulnerando el principio de veracidad. Los datos han de responder a lo que dicta la realidad. El problema que se plantea en este punto es que en el ámbito sanitario la realidad puede ser

[1283] Resolución de la AEPD, R/01879/2008, de 17 de diciembre de 2008, procedimiento PS/00380/2008.

interpretada de muy diferentes maneras. Un paciente que pide opiniones diferentes sobre una circunstancia determinada puede recibir distintas interpretaciones sobre ese mismo hecho. En este caso, si se descubre que una de las interpretaciones es errónea se encontrará con que los datos que contiene la HC no responden a la verdad: por ejemplo, que se haya diagnosticado una enfermedad a un enfermo cuando ese hecho es falso. Cuando este dato es conocido y todavía se mantiene la interpretación errónea, entonces sí puede decirse que se falta al principio de veracidad.

B) Hay que tener en cuenta que la información sanitaria es una información con un alto grado de tecnicismo. Esto hace que en muchas ocasiones el paciente no esté capacitado por sí mismo para comprender la información que se refiere a su persona y obliga a que haya que tener mucha cautela a la hora de alterar o cambiar la información sanitaria. En el ejercicio de acceso, rectificación y cancelación de la información sanitaria por parte de los pacientes, este último tendrá que estar, en la mayoría de supuestos, asistido por los propios profesionales sanitarios.

A esta circunstancia hay que añadirle que los documentos administrativos, las historias clínicas entre ellas, gozan de la presunción de veracidad. La LPAC les reconoce este efecto[1284], por lo que para que la rectificación de dichos documentos se pueda llevar a cabo hará falta, que el titular de los datos pueda demostrar que los datos que posee la Administración son inexactos. Es lo que parecía desprenderse también del anterior reglamento que desarrollaba la LORTAD[1285] y lo que ha confirmado la jurisprudencia[1286].

Así, si se tiene en cuenta que tratándose de información sensible y técnica el acceso, la rectificación y la cancelación de los datos de carácter personal relativos a la salud de las personas habrá de hacerse bajo supervisión de profesionales sanitarios, y que, al ser documentación administrativa, la rectificación y cancelación de esta información a instancia del titular de los datos deberá estar fundamentada en pruebas que justifiquen dicha actuación, podrá concluirse que, en la mayoría de los casos, se establecen garantías suficientes para asegurar que la información relativa a la salud de las personas refleje la realidad a la que se refieren.

C) Por último, el cumplimiento del principio de veracidad plantea un problema práctico de envergadura en el ámbito sanitario. El principio exige para su cumplimiento el ejercicio por parte del titular de los datos de los derechos de acceso, de rectificación y cancelación. Si el titular no tiene acceso a la información no podrá conocer si es veraz o no. Como se verá más adelante, el ejercicio de este derecho por parte del paciente ha traído un profundo debate en torno a quién es el propietario real de dicho documento.

[1284] Artículo 57.1 LPAC: "*Los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa*".
Artículo 46.4 LPAC: "*Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas"*.

[1285] Artículo 15.1 RD 1332/1994: "*Cuando el acceso a los ficheros revelare que los datos del afectado son inexactos o incompletos, inadecuados o excesivos, podrá éste solicitar del responsable del fichero la rectificación o, en su caso, cancelación de los mismos*.
No obstante, cuando se trate de datos que reflejen hechos constatados en un procedimiento administrativo, aquéllos se considerarán exactos siempre que coincidan con éste".

[1286] SAN 28 de febrero 2007, FJ 3.

En algunas ocasiones se ha subrayado que el titular de los datos no tiene derecho a acceder a la historia clínica completa debido a que en ella constan anotaciones subjetivas del profesional que este último no quiere que sean vistas. Se ha comentado que dicho acceso indiscriminado al documento sanitario por parte del paciente conllevaría que el profesional dejase de redactar dichos apuntes subjetivos. La propia normativa sanitaria se ha hecho eco de esta circunstancia[1287]. A este argumento se opone, sin embargo, el hecho de que los datos contenidos en dicho documento, incluso las anotaciones subjetivas, se refieren al paciente y que éste debería tener acceso a toda la información que a él se refiere. Basta decir en este momento que en el acceso a la historia clínica confluyen diferentes intereses que hay que tener en cuenta y que han de ponerse en relación para determinar hasta donde alcanza el derecho de acceso del titular de los datos[1288].

Desde el punto de vista del principio de veracidad habría que posibilitar el completo acceso del titular de los datos a la historia clínica, a no ser que dicho ejercicio haya de ser limitado para salvaguardar la salud de esa u otra persona, es decir, por motivos terapéuticos[1289]. Evidentemente, el propio titular de los datos podrá determinar si unos datos son o no veraces, pero para ello necesariamente ha de tener acceso a la documentación sanitaria. Hay que tener en cuenta lo que se dijo en el comienzo de este apartado: el cumplimiento del principio de veracidad es esencial para llevar a cabo los fines que el responsable del fichero pretende. En este sentido, podría pensarse que para ambas partes resultaría de interés el acceso del titular de los datos a la historia clínica.

[1287] Artículo 18.3 LBAP: "*El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse (...) en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas*".

[1288] BELTRÁN, COLLAZO, GERVÁS, GONZÁLEZ SALINAS, GRACIA, JÚDEZ, RODRÍGUEZ SENDÍN, RUBÍ, SÁNCHEZ, *Guías de Ética...*, cit., 2005, pp. 63-66.

[1289] Artículo 5.4 LABP: "*El derecho a la información sanitaria de los pacientes puede limitarse por la existencia de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho*".

CAPÍTULO 4. EL CONSENTIMIENTO INFORMADO.

Los principios básicos que determinan la calidad de los datos, y en particular el principio de finalidad, constituyen uno de los pilares de la regulación de la protección de los datos de carácter personal. Junto a estas figuras, y en el mismo nivel de relevancia, es decir, en el núcleo del derecho a la autodeterminación informativa, se encuentra otro principio: "el consentimiento informado". Sin duda alguna se erige en la principal facultad de control sobre los datos de carácter personal[1290]. Al estudio de esta figura se dedicará el apartado siguiente.

I CONCEPTO E IMPORTANCIA DEL CONSENTIMIENTO INFORMADO COMO EXPRESIÓN DE LA AUTONOMÍA DE LAS PERSONAS.

I.1. El principio de autonomía como fundamento del consentimiento informado.

I.1.1. Introducción a la relación entre el consentimiento informado y el principio de autonomía.

El consentimiento informado reconoce la capacidad del titular de los datos de autorizar o no un determinado tratamiento de los mismos. Esta institución constituye la principal facultad de control que los ciudadanos tienen sobre la información que les concierne. En este sentido la jurisprudencia ha considerado que el consentimiento informado pertenece al que denomina contenido esencial del derecho a la autodeterminación informativa[1291], y ha subrayado el papel de dicho consentimiento como facultad nuclear de este derecho, en la medida que supone situar el centro de decisión de lo que va a suceder con los datos de carácter personal en el titular de los mismos[1292]. Es más, esta misma jurisprudencia en más de una ocasión ha equiparado, aunque sea a nivel conceptual, el consentimiento informado y el derecho a la autodeterminación informativa entendiéndolos como sinónimos[1293]. No hace falta decir que el derecho a la autodeterminación informativa reconoce o engloba más elementos que el consentimiento. Sin embargo, esta equiparación ayuda a comprender hasta qué punto esta figura se erige en piedra angular del derecho a la autodeterminación informativa.

Así, la máxima de la que parte la Ley es que para manipular los datos de cada persona, en principio, hará falta su aceptación o aprobación. El individuo puede disponer de los datos que pueden vincularse de forma directa o indirecta a su persona. El consentimiento informado reconoce, en gran medida, la capacidad de disponer de un aspecto de la vida que corresponde a cada individuo, en este caso de los datos que a cada uno conciernen.

Precisamente esa facultad de disponer de lo que corresponde a cada uno no es otra cosa que el reconocimiento del principio de autonomía. Sin duda alguna el consentimiento informado es expresión de este principio[1294]. La vinculación entre ambos elementos en el ámbito de la protección de datos es clara: el consentimiento informado tiene su fundamento en el reconocimiento de la autonomía de los individuos. Partiendo de la consideración de que las

[1290] SAN 18 julio 2007, FJ 3.
[1291] STC 30 de noviembre 2000, FJ 2.
[1292] SAN 17 abril 2007, FJ 3.
[1293] SAN 12 enero 2007, FJ 5.
[1294] CANTERO MARTÍNEZ, *La Autonomía...,* cit., 2005, p. 11.

personas, cuando están debidamente informadas y en posesión plena de sus facultades, están capacitadas para tomar decisiones sobre los asuntos que les incumben, se reconoce el principio de autonomía: la facultad de decidir libremente sobre las cuestiones propias de cada uno[1295]. La capacidad de autorizar o no un tratamiento determinado de datos de carácter personal es expresión de ese derecho a la autodeterminación.

I.1.2. El consentimiento informado y el principio de autonomía en el tratamiento sanitario.

La vinculación entre el consentimiento informado y el principio de autonomía constituye una ecuación que ha sido analizada en un sector tan complejo como el sanitario. Así pues, para comprender adecuadamente la consideración del principio de autonomía como fundamento del consentimiento informado en el ámbito de la protección de datos hay que analizar necesariamente la relación existente entre estas dos figuras en el sector de la sanidad.

El principio de autonomía ha sido estudiado con gran profundidad en el ámbito del derecho sanitario. Se podría entender este principio como la facultad de las personas de determinar qué es lo que quieren hacer con su salud. En el ámbito internacional una de las primeras declaraciones expresas sobre la importancia del principio de autonomía en este sector se da en Estados Unidos en 1914[1296]. En el ámbito estatal a lo largo de los años se ha ido otorgando cada vez mayor importancia a este concepto hasta que a partir, fundamentalmente, de la aprobación de la LBAP[1297], que considera la autonomía del paciente como uno de los principios que han de guiar en todo momento la actividad sanitaria[1298], se ha consolidado definitivamente, cuando menos en teoría, como inspirador de la relación entre paciente y profesional sanitario. Expresión clara de esta consolidación es la inclusión en la norma citada de la figura de las instrucciones previas[1299], a través de la cual una persona mayor de edad y capacitada puede decidir en un determinado momento qué hacer con su salud en un futuro, para el supuesto en que en dicho estadio futuro, debido a su estado de salud, no esté capacitada para tomar esa decisión[1300].

La consolidación de la autonomía como principio inspirador de toda actuación en el campo sanitario es un hecho hoy por hoy constatable. La incorporación de este principio al esquema de

[1295] LORDA, *El Consentimiento...*, cit., 2000, pp. 178-183; DE LA VEGA-HAZAS RAMÍREZ, "Autonomía, dos...", cit., 2000, p. 195: desde el punto de vista etimológico "Autonomía significa capacidad de otorgarse la Ley a uno mismo".

[1296] TARODO SORIA, "La doctrina...", cit., 2006, pp. 232-233, se refiere al conocido caso *Schloendorff v. The Society of the New York Hospital*.

[1297] La LBAP se fundamenta sustancialmente en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y la Dignidad del ser Humano con respecto a las aplicaciones de la Biología y la Medicina de 4 de abril de 1997, (Convenio de Oviedo relativo a los derechos humanos y la biomedicina).

[1298] Artículo 2.1 LBAP: la "*dignidad de la persona humana, el respeto a la autonomía de su voluntad y a su intimidad orientarán toda la actividad encaminada a obtener, utilizar, archivar, custodiar y transmitir la información y la documentación clínica"*.

[1299] MÉJICA y DÍEZ , *El Estatuto...*, cit., 2006, p. 133 y siguientes.

[1300] Artículo 11.1 LBAP: "*Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas"*.

funcionamiento del sistema sanitario ha supuesto un cambio de importancia. Como se ha subrayado por la mayoría de los autores que han analizado esta relación, el reconocimiento de la autonomía ha constituido el abandono del ya superado principio de beneficencia[1301]. Este último principio guiaba la actuación del profesional con el paciente y llevaba a una relación paternalista[1302], en la que el paciente se sometía a lo que dictaba el profesional sanitario, que era el que poseía el conocimiento y la información[1303]. Con el reconocimiento del principio de autonomía se deja a un lado la relación estrictamente vertical entre médico y paciente, en la que el paciente básicamente se limita a obedecer al médico[1304]. Así, en la actualidad se establece una relación horizontal donde el paciente participa activamente de la toma de decisiones que le afectan[1305]. Este último no acude al centro sanitario para dejar sus problemas en manos exclusivas del profesional y que éste actúe de forma unilateral, sino que acude para tomar las decisiones por sí mismo con la colaboración y asistencia de dichos profesionales. Se tiene que partir de la idea de que el paciente es adulto y que, cuando está debidamente informado, está capacitado para tomar sus propias decisiones sobre su salud.

Siendo esto así, cabe preguntarse si se puede llegar a comprender el principio de autonomía como una forma de tomar las decisiones de manera individual sin la intervención de terceras personas. ¿Se puede entender que ha de ser el paciente el único en determinar el tipo de tratamiento que ha de administrársele? Desde el ámbito de la filosofía ya se ha advertido más de una vez que el sentido del principio de autonomía no puede llevarse al extremo, pues conllevaría un individualismo exacerbado e incluso peligroso para la propia persona[1306]. Si se hace referencia al principio en sentido genérico, hay que entenderlo como la capacidad de los individuos de ser dueños de sus propios destinos sin que haya intromisiones de terceras personas no permitidas[1307]. No obstante, si bien hay que interpretarlo de la forma citada, no se puede escapar a la idea de que en el ámbito estrictamente sanitario la autonomía no puede ser comprendida en términos absolutos. En un espacio tan especializado y tan técnico como el que se está tratando es indispensable que el profesional sanitario tenga un papel fundamental a la hora de tomar decisiones. Hay que tener en cuenta que el sujeto no siempre estará capacitado para decidir de la manera más acertada y que en determinadas circunstancias la intervención de una tercera persona será necesaria para adoptar la mejor opción[1308]. Así, la autonomía no se comprende, como ha apuntado algún autor, como la facultad de tomar la decisión unilateralmente por el paciente, sino como un ejercicio de colaboración entre éste y el médico[1309]. Es decir, la relación médico-paciente ha de interpretarse como un equilibrio entre el principio de autonomía y

[1301] CANTERO MARTÍNEZ, *La Autonomía...*, cit., 2005, p. 8.
[1302] SEOANE RODRÍGUEZ, "El Significado...", cit., 2004, pp. 42-46, entiende como paternalismo el "decidir por y sobre el otro sin el otro (sin tomar en consideración al otro)".
[1303] RODRÍGUEZ LÓPEZ, *La Autonomía...,* cit., 2004, p. 14; HIPATIA, *Dos para…,* cit., 2004, p. 23.
[1304] LORDA, *El Consentimiento...*, cit., 2000, p. 26-29.
[1305] MARTÍNEZ AGUADO, "Aspectos Éticos...", cit., 2002, pp. 77 y 83.
[1306] MARTÍNEZ MUÑOZ, "Autonomía...", cit., 2007, pp. 746-751.
[1307] GONZÁLEZ AMUCHÁSTEGUI, *Autonomía, Dignidad y Ciudadanía...,* cit., 2004, pp. 373-375.
[1308] GONZÁLEZ AMUCHÁSTEGUI, *Autonomía, Dignidad y Ciudadanía...,* cit., 2004, p. 387.
[1309] SEOANE, "El Significado...", cit., 2004, p. 43-45, subraya la idea de que la autonomía no se entiende como el hecho de "decidir por y sobre uno mismo sin los otros (sin considerar los otros)", sino como, "decidir por y sobre uno mismo con los otros (tomando en consideración a los otros)".

el paternalismo bien entendido[1310]. En definitiva, no se trata de entender el principio de autonomía en un sentido estricto y radical[1311], sino simplemente de comprender que el paciente está capacitado, cuando se le informa adecuadamente, para participar junto a los demás agentes en la toma de decisiones que afectarán a su salud. Se fija así una relación más democrática en la que la participación de ambos sujetos es necesaria.

Pues bien, el instrumento a través del que se expresa el principio de autonomía que se acaba de comentar no es otro que el del consentimiento informado[1312]: el médico informa al paciente de las posibilidades que hay en una determinada situación, y de las ventajas y desventajas de cada una, y le ayuda a tomar una decisión que en última instancia, salvo circunstancia excepcional, deberá adoptar el paciente. Cierto es que la figura del consentimiento informado ha planteado en este ámbito numerosos problemas en la práctica; no hay más que ver el gran número de denuncias que se interponen ante los Tribunales en relación a esta cuestión. No obstante, es indudable que esta prerrogativa se considera en la actualidad una de las herramientas más importantes para llevar a cabo la asistencia médica[1313]. La jurisprudencia ha llegado a calificar el consentimiento informado en este ámbito como derecho humano fundamental[1314]. Si bien esta afirmación ha sido cuestionada por parte de la doctrina[1315], la gran relevancia del consentimiento informado queda patente en el hecho de que en la normativa dirigida a regular la realidad sanitaria, tanto la estatal como la autonómica, ha ido adquiriendo una presencia cada vez mayor[1316]. En este sentido la aprobación de la LBAP se considera un hito de importancia en la medida en que reconoce expresamente el consentimiento informado y el principio de autonomía como elementos vertebradores de la relación médico-paciente[1317].

La relevancia que se da a esta figura en el campo sanitario está más que justificada y es que a través del consentimiento informado se encauza la participación del paciente en el tratamiento de su enfermedad. Éste, en el ejercicio del consentimiento informado, conoce todos los elementos que caracterizan a una enfermedad, patología o estado concreto, las ventajas y desventajas de los diferentes tratamientos que se pueden llevar a cabo, y toma una decisión al respecto. Con lo dicho queda clara la relación entre el principio de autonomía y el derecho al consentimiento informado.

Hay que tener presente que lo que se protege en última instancia con el reconocimiento del principio de autonomía y del consentimiento informado no es otra cosa que la dignidad de las personas y el libre desarrollo de la personalidad[1318]. Así lo han entendido la doctrina, basándose en la legislación,[1319] y la jurisprudencia[1320]. La dignidad, que podría entenderse como “un valor

[1310] GONZÁLEZ AMUCHÁSTEGUI, *Autonomía, Dignidad y Ciudadanía...,* cit., 2004, pp. 390-391.
[1311] APARISI MIRALLES, “El significado...”, cit., 2004, p. 112.
[1312] LIZARRAGA BONELLI, “La información...”, cit., 2004, p. 232; RODRÍGUEZ LÓPEZ, *La Autonomía...*, cit., 2004, p. 116; CANTERO MARTÍNEZ, *La Autonomía...,* cit., 2005, p. 7; ROMEO CASABONA, *Información y...,* cit., 2000, p. 12.
[1313] IBARZABAL, “Bioética: tomando...”, cit., 2004, p. 163.
[1314] STS 12 de enero 2001, FJ 1.
[1315] MÉJICA y DÍEZ, *El Estatuto...,* cit., 2006, p. 50.
[1316] MÉJICA y DÍEZ, *El Estatuto...,* cit., 2006, pp. 39-47.
[1317] GARCÍA ORTEGA, CÓZAR MURILLO, y ALMENARA BARRIOS, “La autonomía...”, cit., 2004, pp. 470-471.
[1318] APARISI MIRALLES, “El significado...”, cit., 2004; RODRÍGUEZ LÓPEZ, *La Autonomía...*, cit., 2004, p. 118.
[1319] APARISI MIRALLES, “El significado...”, cit., 2004, p. 80.

espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás"[1321], podría verse menoscabada, o cuando menos cuestionada, en el caso de que al paciente se le reconociese simplemente un papel de mero espectador en el proceso de toma de decisiones que le afectan directamente. El hecho de ser conscientes de nuestro propio ser, y de querer disponer de él y desarrollarlo según el criterio de cada uno, necesariamente tiene que venir acompañado del reconocimiento del principio de autonomía[1322] y del derecho al consentimiento informado como expresión concreta del mismo[1323].

Desde un punto de vista más práctico, con la consagración del binomio autonomía-consentimiento informado se pretende crear un vínculo de confianza mutua entre médico y paciente, de tal forma que las decisiones se adopten con la colaboración de ambos sujetos[1324]. La inclusión en el ámbito sanitario del principio de autonomía ha llevado a la comprensión de la relación médico-paciente de forma diferente a como se ha entendido hasta ahora.

Por un lado, el profesional sanitario ha de ser consciente del cambio que supone aceptar la participación del paciente en el proceso sanitario[1325]. La tarea de informar al paciente y de solicitar su consentimiento supone un trabajo añadido para el profesional frente a la posibilidad de hacer, simplemente, lo que su criterio y conocimiento le dicta, sin tener que contar con el usuario. Pues bien, esta tarea no tiene que implicar para el profesional, como se ha entendido en algún momento[1326], una carga burocrática, una cuestión meramente formal que le ha sido impuesta desde el mundo del derecho[1327]. Debería suponer el fortalecimiento de su relación con el paciente[1328]. Por otro lado, el paciente no puede entender este instrumento como un arma

[1320] STS 21 de diciembre 2006, FJ 3.
[1321] STC 11 de abril de 1985, FJ 8.
[1322] STS 11 de mayo de 2001, FJ 7: "Asimismo, se ha expuesto que «...la información del médico preceptiva para que el enfermo pueda escoger en libertad dentro de las opciones posibles que la ciencia médica le ofrece al respecto e incluso la de no someterse a ningún tratamiento, ni intervención, no supone un mero formalismo, sino que encuentra fundamento y apoyo en la misma, en la exaltación de la dignidad de la persona que se consagra en su artículo 10,1, pero sobre todo, en la libertad, de que se ocupan el art. 1,1 reconociendo la autonomía del individuo para elegir entre las diversas opciones vitales que se presenten de acuerdo con sus propios intereses y preferencias".
[1323] STS 11 de mayo de 2001, FJ 7: "El consentimiento informado constituye un derecho humano fundamental, precisamente una de las últimas aportaciones realizada en la teoría de los derechos humanos, consecuencia necesaria o explicación de los clásicos derechos a la vida, a la integridad física y a la libertad de conciencia. Derecho a la libertad personal, a decidir por sí mismo en lo atinente a la propia persona y a la propia vida y consecuencia de la autodisposición sobre el propio cuerpo, regulado por la Ley General de Sanidad y actualmente también en el Convenio Internacional para la Protección de los Derechos Humanos y la Dignidad del Ser Humano con respecto a las Aplicaciones de la Biología y de la Medicina y que ha pasado a ser derecho interno español por su publicación en el BOE forma parte de la actuación sanitaria practicada con seres libres y autónomos»".
[1324] SAN JULIÁN PUIG, "Los Principios...", cit., 2004, pp. 60-62.
[1325] BLAS ORBAN, *El equilibrio...*, cit., 2006, p. 32; SAN JULIÁN PUIG, "Los Principios...", cit., 2004, p. 57.
[1326] BLAS ORBAN, *El equilibrio...*, cit., 2006, pp. 107-109.
[1327] SAN JULIÁN PUIG, "Los Principios...", cit., 2004, pp. 58-59.
[1328] DE LORENZO Y MONTERO y SÁNCHEZ CARO, "Consentimiento Informado", cit., 1999, p. 209; ROMEO CASABONA, *Información y...,* cit., 2000, p. 12: sobre el consentimiento informado: "no se trata de una imposición más del ordenamiento jurídico o de una secuela de esa "reciente" impregnación "bioética" de todo lo médico, como si se pretendiera sobrecargar la ya por lo general muy apretada lista de obligaciones que tienen que ir satisfaciendo particularmente los médicos. Al contrario, se trata de una especie de contrapartida al paciente, de uno de los presupuestos para el ejercicio de su propia autonomía en un ámbito de su vida personal que en no pocas ocasiones puede llegar a ser de extraordinaria trascendencia para él y su entorno".

arrojadiza con la que cuenta para atacar la actuación de los profesionales y de la que puede beneficiarse[1329]. En definitiva, el consentimiento informado tiene que ser interpretado como un valor que enriquece la relación entre profesional y usuario[1330]. En este sentido, para encontrar el valor añadido que supone el respeto a la institución del consentimiento informado como concreción del principio de autonomía, hay que tratar de buscar el equilibrio entre el respeto al principio de autonomía y la salvaguarda de la agilidad que requiere el ejercicio de una profesión tan compleja como la sanitaria[1331].

I.1.3. El consentimiento informado y el principio de autonomía en la protección de datos.

Las consideraciones que se acaban de hacer sobre la relación entre el consentimiento informado y el principio de autonomía en el ámbito sanitario son trasladables, con matices, a la institución del consentimiento informado reconocida en el ámbito de la protección de datos de carácter personal. Así lo ha visto también la jurisprudencia[1332]. La relación de ambas figuras en cada uno de los citados sectores, sin embargo, presenta ciertas particularidades.

A la hora de analizar esas diferencias habrá que observar el vínculo entre el principio de autonomía y el consentimiento informado desde dos perspectivas diferentes. En primer lugar, entendiendo el consentimiento informado como expresión principal del principio de autonomía, autodeterminación informativa en este caso. Y en segundo lugar, entendiendo el consentimiento informado en el ejercicio del derecho a la autodeterminación informativa en el ámbito concreto de la sanidad, como vía para reforzar la relación entre el profesional sanitario y el paciente o usuario.

A) Desde el primer punto de vista, no parece haber duda de que el fundamento del consentimiento informado en el ámbito de la protección de datos se encuentra también, en última instancia, en el principio de autonomía. El hecho de que el derecho fundamental que aquí se trata haya sido calificado como derecho a la autodeterminación informativa es ciertamente revelador. El derecho a la protección de datos no es otra cosa sino la facultad de controlar uno de los aspectos que componen la personalidad del individuo: el de los datos de carácter personal. Sin necesidad de entrar a analizar con detalle la esencia del derecho a la autodeterminación informativa[1333], se puede concluir que en el ejercicio de este derecho fundamental se advierte con mayor intensidad que en el caso de otros derechos el ejercicio de la autonomía de las personas. Frente a derechos que como el de la intimidad tratan de preservar un ámbito de libertad de los individuos al que terceras personas no pueden acceder, el derecho a la autodeterminación informativa no reconoce sólo ese aspecto, sino también facultades positivas, de hacer[1334], que expresan mejor la esencia del principio de autonomía, pues constituyen la posibilidad de ejercer directa y activamente la misma. Se trata de convertir esa autonomía en acciones determinadas

[1329] CANTERO MARTÍNEZ, *La Autonomía...*, cit., 2005, pp. 85-87; BLAS ORBAN, *El equilibrio...*, cit., 2006, p. 29.
[1330] RODRÍGUEZ LÓPEZ, *La Autonomía...*, cit., 2004, pp. 33-34.
[1331] RODRÍGUEZ LÓPEZ, *La Autonomía…,* cit., 2004, p. 25.
[1332] SSTS, 26 de noviembre de 2004, FJ 3; 18 de junio de 2004, FJ 1; 4 de abril de 2000.
[1333] MURILLO DE LA CUEVA, *El Derecho a la Autodeterminación...,* cit., 1990.
[1334] STC 30 de noviembre del 2000, FFJJ 5 y 6.

como consentir, o acceder, o rectificar, o cancelar. El individuo controla activamente lo que le corresponde como persona, en este caso, los datos de los que es titular.

El derecho a la autodeterminación informativa es, por lo tanto, expresión de la autonomía de las personas y se fundamenta en última instancia en la dignidad de las mismas. Si la dignidad consiste en la autoconsciencia sobre la vida y el ser de cada uno, la protección de datos de carácter personal no es otra cosa que el derecho a controlar parte de esa identidad, la facultad de ejercer la autonomía sobre un aspecto concreto de nuestro ser. Y precisamente el derecho a consentir o no un tratamiento determinado de los datos que a cada uno corresponden representa una facultad concreta del derecho a la autodeterminación informativa y, en última instancia, de la autonomía y dignidad de cada individuo.

Como se puede apreciar, la relación entre el derecho a otorgar el consentimiento y la autonomía que se da en la protección de datos es, cuando menos, similar a esa misma relación entre el consentimiento y la autonomía que se da en el tratamiento médico o sanitario de las personas. Sin embargo, las consideraciones que se han hecho sobre los efectos de la aplicación del principio de autonomía en la relación médico-paciente han de ser matizadas cuando se tratan de trasponer al ámbito de la protección de datos.

Se ha apuntado que en el sector sanitario el principio de autonomía supone el reconocimiento de la facultad del paciente de tomar decisiones sobre el tratamiento de los problemas que pueda tener en su salud. En este ámbito se establece una relación de confianza, se podría decir que significativamente personal y cercana, entre el profesional y el paciente. Precisamente, lo que trata de conseguir el reconocimiento de la autonomía del paciente es que dicha relación se convierta en más humana. No obstante, también se ha dicho que en la actualidad la relación entre médico y paciente había que plantearla como un equilibrio entre este principio de autonomía y un paternalismo bien entendido. A nadie se le escapa que dentro de esta relación que se comenta el papel del profesional sanitario y el del paciente no es el mismo. La opinión del profesional sanitario, que es quien posee el conocimiento especializado y la información suficiente, juega un papel fundamental en la determinación del camino a seguir por el paciente. Se podría hablar, por lo tanto, de un paternalismo laxo que reconoce e integra la participación del ciudadano en la toma de decisiones

En el campo de la sanidad el consentimiento informado del paciente dependerá en cierto sentido de cómo se haya desarrollado la relación entre médico y paciente. En la mayoría de los casos, sobre todo por la complejidad de la materia[1335], el profesional sanitario se encuentra en una situación de cierta superioridad que hace que pueda guiar y, en cierto sentido, condicionar la decisión del paciente. En el caso de la sanidad el objeto sobre el que se va a dar el consentimiento no es sencillo de delimitar para el paciente: pueden existir diferentes alternativas para un mismo tratamiento; se trata de un ámbito donde la interpretación juega un papel fundamental: interpretación a la hora de realizar el diagnóstico, interpretación a la hora de elegir el tratamiento...; la importancia del bien jurídico último que se protege es especialmente significativa por lo que la cautela puede jugar un papel relevante a la hora de consentir. Esto

[1335] BLAS ORBÁN, *El equilibrio...,* cit., 2006, p. 146.

hace que la ayuda del profesional sanitario sea imprescindible y que la autonomía se vea condicionada por lo que el profesional sanitario pueda opinar o interpretar que es lo más adecuado.

En el caso de la protección de datos de carácter personal, en general, más allá del estricto ámbito sanitario, la relación que se crea entre el titular de los datos de carácter personal y el responsable del fichero, en un inicio, no es idéntica a la que se acaba de plantear. En este campo, en los supuestos en que el consentimiento es requerido, la posición que van a ocupar el titular de los datos y el responsable del fichero será, o debería ser, después de ejercer el derecho a la información, de completa igualdad. El consentimiento informado no se presta sobre una materia tan compleja y técnica como en el sector sanitario, así, es más difícil que dicho consentimiento aparezca condicionado o inducido por una opinión del que solicita dicha aprobación. Aquí, los parámetros que delimitan el objeto sobre el que va a recaer el consentimiento son fáciles de determinar y de comprender por el titular de los datos de carácter personal, por eso la autonomía a la hora de dar el consentimiento en estos casos puede y debe ser plena. De esta manera, se podría plantear como primera diferencia entre ambos consentimientos informados la distinta posición que ocupan en la práctica los sujetos afectados: en el caso de la protección de datos de carácter personal el titular de los datos aparece en una situación o condición más reforzada en comparación a la posición del paciente en la relación médico-paciente. Y se dice que es más reforzada porque su consentimiento estará guiado en mayor medida por su propia voluntad.

De inicio, por lo tanto, en el ámbito de la protección de datos la posición del titular de los mismos y su autonomía se sitúan en una posición más reforzada que cuando se trata de consentir un tratamiento médico. Esta premisa, sin embargo, no se cumple en el ámbito sanitario de manera estricta. Cabe en este momento adelantar un apunte significativo que más adelante será analizado con mayor profundidad, con respecto al consentimiento en el tratamiento de datos sanitarios: la LOPD admite numerosas excepciones al consentimiento informado y, precisamente, cuando se trata de la manipulación de datos sensibles con la finalidad de salvaguardar la salud de las personas, exceptúa la necesidad del consentimiento del titular de los datos empleando términos bastante ambiguos. Así, la exigencia del consentimiento se ve relajada cuando los datos se manipulan con el fin de salvaguardar la salud de la persona. Si bien con matices, en este caso el legislador decide que prevalece la protección de la salud de las personas sobre el derecho a la autodeterminación informativa. De esta manera, el escrupuloso respeto al principio de autonomía que en el ámbito de la protección de datos se da con el reconocimiento del derecho a otorgar el consentimiento informado, se ve negativamente afectado cuando entran en juego intereses o bienes jurídicos dignos de mayor protección, como la salud de las personas.

Esto no sucede por el contrario, no por lo menos en términos tan amplios, cuando se trata del consentimiento informado para llevar a cabo un tratamiento médico. En este último caso, como se verá, la obligación de solicitar la autorización del paciente para realizar la oportuna asistencia sanitaria cuenta con muy pocas excepciones.

B) Desde la segunda perspectiva, se ponía de manifiesto la importancia del consentimiento como instrumento para reforzar la relación entre médico y paciente. En el ámbito sanitario tienen vigencia dos tipos de consentimiento informado, cada uno con sentido propio: el consentimiento informado para el tratamiento sanitario y el consentimiento informado para el tratamiento de los datos de carácter personal. Los dos se encuentran fundamentados en el principio de autonomía pero cada uno con sus características particulares. En todo caso, y esto es lo más relevante, ambas figuras contribuyen a la creación de un mismo elemento: la configuración de una relación de confianza entre el profesional sanitario y el paciente. El consentimiento informado para el tratamiento sanitario posibilita la participación del paciente en la determinación del proceso médico al que se le ha de someter. Por ello, se decía, no puede considerarse por parte de los profesionales sanitarios esta operación como un mero acto burocrático. Y el consentimiento informado para el tratamiento de los datos de carácter personal permite que el paciente tenga conocimiento de lo que se hace con la esfera de su vida que constituyen los datos de carácter personal sanitarios y así poder ejercer las facultades que le corresponden como titular de dichos datos. Por ello, tampoco esta operación puede entenderse por los profesionales sanitarios como un mero formalismo.

En este sector, los dos tipos de consentimiento que se acaban de señalar se integran en la misma relación que vincula a la Administración sanitaria, en general, con el paciente o usuario. Como se verá, ambos se dirigen, aunque por diferentes vías, a fortalecer la figura del paciente y su autonomía o autodeterminación frente a decisiones que pueden afectarle. Ambas instituciones tratan de humanizar la citada relación con el fin último de mejorar la protección de la salud de las personas.

El respeto del principio de autonomía en estas dos vertientes, marcadas por las dos formas del consentimiento informado, viene a contribuir a que se promueva la participación del paciente en la toma de decisiones que le afectan. Esta circunstancia conllevará que exista una relación adecuada, de confianza, entre profesional sanitario y paciente[1336], en la que el intercambio de información sea constante y se realice de manera continuada y segura[1337]. En última instancia, todo ello redundará en que la salud de los individuos quede protegida de la mejor manera posible.

I.2. Concepto de consentimiento informado. Definición y relación entre los elementos que lo componen: la información y el consentimiento.

Tanto en el derecho médico como en las normas dirigidas a regular la protección de datos de carácter personal pueden encontrarse definiciones, con mayor o menor precisión, de este derecho. Como es sabido, también el derecho civil reconoce esta figura al analizar instituciones como el contrato[1338]: el consentimiento constituye el elemento principal en la formulación de un contrato[1339]. Diferentes ámbitos se refieren al consentimiento informado. No obstante, basta para

[1336] LOSCERTALES ABRIL y GÓMEZ GARRIDO, *La Comunicación...*, cit., 1999, p. 66.
[1337] GÓMEZ ESTEBAN, *El Médico...*, cit., 2002, pp. 60 y 69.
[1338] Artículo 1.262 CC: "*El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato*".
[1339] SAN JULIÁN PUIG, *El Objeto...*, cit., 1996, p. 33.

los objetivos de este estudio con exponer una definición genérica, con el fin de determinar después las características particulares que ha de recoger en el ámbito de la protección de datos.

En la normativa sanitaria, tanto desde el ámbito autonómico como estatal, se ha tratado el consentimiento resaltando su importancia como expresión del principio de autonomía[1340]. En algún caso, incluso se ha dado una definición expresa de lo que se entiende por esta figura[1341]. Hay que subrayar la aportada por la LBAP que la define como "*la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud*"[1342]. La jurisprudencia que ha analizado las características del consentimiento informado en el ámbito sanitario ha dado también algunas aclaraciones sobre lo que se ha de entender por dicha institución. Subrayando su relevancia como vehículo con el que cuentan las personas para decidir sobre su salud[1343], en alguna ocasión ha llegado a dar una definición relativamente completa, así: "El consentimiento informado es (...) presupuesto y elemento esencial de la *lex artis* y como tal forma parte de toda actuación asistencial (...) constituyendo una exigencia ética y legalmente exigible a los miembros de la profesión médica (...). Es un acto que debe hacerse efectivo con tiempo y dedicación suficiente y que obliga tanto al médico responsable del paciente, como a los profesionales que le atiendan durante el proceso asistencial, como uno más de los que integran la actuación médica o asistencial, a fin de que pueda adoptar la solución que más interesa a su salud. Y hacerlo de una forma comprensible y adecuada a sus necesidades, para permitirle hacerse cargo o valorar las posibles consecuencias que pudieran derivarse de la intervención sobre su particular estado, y en su vista elegir, rechazar o demorar una determinada terapia por razón de sus riesgos e incluso acudir a un especialista o centro distinto"[1344]. Luego sigue diciendo: "El consentimiento (...) es un *acto de voluntad* que ha de ser *claro e inequívoco* aunque no importe la forma (expresa o tácita) entendiéndose que hay consentimiento incluso cuando se realizan ciertos actos llamados <<*concluyentes*>> *(facta concluentia)* como puede ser el silencio. A su vez, el consentimiento ha de ser libre y conscientemente emitido y manifestado, es decir sin vicio que lo invalide. Supone (...) una voluntad concorde, acto humano que del interior (motivación, deliberación y decisión) aflora al exterior, se <<manifiesta>>, produciéndose,

[1340] Artículo 6 Ley 21/2000, 29 de diciembre, Cataluña, sobre los Derechos de Información concernientes a la Salud y la Autonomía del Paciente, y la Documentación Clínica; Artículo 28 Ley 8/2003, 8 de abril, Castilla y León, sobre derechos y Deberes de las Personas en relación con la Salud;

[1341] Artículo 3.1 Ley 3/2001, 28 de mayo, de Galicia, reguladora del Consentimiento Informado y de la Historia Clínica de los Pacientes, reformada por la Ley 3/2005, 7 de marzo: "*A los efectos de esta Ley se entiende por consentimiento libre el prestado libre y voluntariamente por el afectado para toda actuación en el ámbito de su salud y una vez que, recibida la información adecuada, hubiera valorado las opciones propias del caso. El consentimiento será verbal por regla general, y se prestará por escrito en los casos de intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores, y, en general, en la aplicación de procedimientos que supongan riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente"*. Artículo 8.1 Ley 1/2003, 28 de enero, Valencia, De Derechos e Información al Paciente de la Comunidad Valenciana: "*Se entiende por consentimiento informado la conformidad expresa del paciente, manifestada por escrito, previa la obtención de la información adecuada con tiempo suficiente, claramente comprensible para él, ante una intervención quirúrgica, procedimiento diagnóstico o terapéutico invasivo y en general siempre que se lleven a cabo procedimientos que conlleven riesgos relevantes para la salud*".

[1342] Artículo 3 LBAP.

[1343] SSTS 23 de mayo de 2007, FJ 3 y 4 de abril de 2000, FJ 3.

[1344] STS 15 noviembre de 2006, FJ 2.

al aunarse con otra voluntad ajena, el concurso de la oferta y de aceptación"[1345]. Por su parte, la doctrina que se ha dedicado a analizar las consecuencias que derivan del reconocimiento de la autonomía del paciente, ha dado también numerosas definiciones de esta figura[1346], si bien, prácticamente todas coinciden en resaltar los mismos aspectos que citan la Ley y la jurisprudencia.

La normativa dedicada a regular el derecho a la autodeterminación informativa también da una definición de este concepto. La LOPD, siguiendo lo que determina la Directiva europea reguladora de la protección de datos[1347], entiende que el consentimiento es la "*manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen*"[1348]. Esta misma definición es la que se recoge en las normas autonómicas reguladoras de la protección de datos de carácter personal[1349] y en el reglamento que desarrolla la Ley estatal hoy vigente[1350]. La jurisprudencia que analiza los diferentes problemas que se han generado en torno a la protección de datos de carácter personal, por su parte, se ha limitado en la mayoría de casos a reproducir la definición dada por la Ley. No obstante, en muchas de las resoluciones se resalta la importancia del consentimiento informado como vía para que sea el titular de los datos el que determine los parámetros en los que se han de tratar los datos de carácter personal que le conciernen[1351].

Teniendo en cuenta lo que se ha dicho hasta ahora, sobre todo en lo relativo a las definiciones dadas del consentimiento informado en el ámbito sanitario, se podría concluir que

[1345] LIZARRAGA BONELLI, "La Información...", cit., 2004, pp. 231-232, haciéndose eco de distintas sentencias del TS: 14 junio de 1963 y 7 diciembre de 1996, fundamentalmente.

[1346] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...,* cit., 1999, p. 194, recogen estas palabras de Diego Gracia: el consentimiento informado en el ámbito estricto de la sanidad constituye, según se ha repetido muchas veces por la doctrina, "una de las máximas aportaciones que la ciencia jurídica ha realizado a la medicina"; GÓMEZ DE ARRIBA, *El Consentimiento...*, cit. 2001, hace suya esta definición dada por Cesar Galán: el consentimiento informado es "el proceso gradual que tiene lugar en el seno de la relación sanitario-usuario, en virtud del cual el sujeto competente o capaz recibe del sanitario información bastante, en términos comprensibles, que le capacita para participar voluntaria, consciente y activamente en la adopción de decisiones respecto al diagnóstico y tratamiento de su enfermedad"; RODRÍGUEZ LÓPEZ, *La Autonomía...*, cit. 2004, p. 69, en el mismo sentido señala que "se entiende por consentimiento informado, el proceso que surge en la relación médico/paciente, por el cual el paciente expresa su voluntad y ejerce por tanto su libertad al aceptar someterse o rechazar un plan, diagnóstico, terapéutico, de investigación, etc., propuesto por el médico para actuar sobre su persona y todo ello tras haber recibido información suficiente sobre la naturaleza del acto o actos médicos, sus beneficios y riesgos, y las alternativas que existan a la propuesta". Este último autor recoge también la definición dada en el Manual de Ética de 1984 por el Colegio de Médicos Americanos: *<<El CI consiste en la explicación, a un paciente atento y mentalmente competente, de la naturaleza de su enfermedad, así como del balance entre los efectos de la misma y los riesgos y beneficios de los procedimientos terapéuticos recomendados, para a continuación solicitarle su aprobación para ser sometido a esos procedimientos. La presentación de la información al paciente debe ser comprensible y no sesgada; la colaboración del paciente debe ser conseguida sin coerción; el médico no debe sacar partido de su potencial dominancia psicológica sobre el paciente>>".*

[1347] Artículo 2.h) Directiva 95/46/CE.

[1348] Artículo 3.h) LOPD.

[1349] Artículo 3.g) Ley 2/2004, 25 de febrero, del País Vasco, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos; y Artículo 3.h), Ley 8/2001, 13 de julio, de la Comunidad de Madrid, de Protección de Datos de carácter personal de la Comunidad de Madrid.

[1350] Artículo 5.1.d) RDLOPD.

[1351] SAN 27 febrero 2003, FJ 4: el consentimiento informado "se traduce en que es la persona titular de los datos la que debe determinar el nivel de protección de sus datos, y, por lo tanto, a ella corresponde determinar el alcance con el que sus datos pueden ser utilizados".

esta figura constituye una institución a través de la cual un sujeto capaz, o, en su caso, su representante, autoriza, consciente y voluntariamente, de una manera clara, la manipulación de los datos que le conciernen, después de haber sido informado clara y suficientemente sobre los distintos aspectos que van a rodear dicha manipulación. Los diferentes aspectos que completan la definición serán analizados al estudiar de manera individualizada el consentimiento y el derecho a recibir información.

Se deduce de la definición que se ha dado que el consentimiento informado se compone de dos elementos fundamentales: el consentimiento y el derecho a ser informado.Si bien cada uno tiene sentido propio, lo cierto es que alcanzan su pleno significado cuando se reconocen de manera conjunta[1352]. En el sector sanitario esta cuestión ha sido puesta de manifiesto claramente en la normativa[1353].

La autorización por parte del paciente para que un tratamiento pueda ser llevado a cabo sólo podrá darse cuando ha sido previamente informado de forma pertinente, de tal manera que conozca todos los elementos del objeto consentido[1354]. En el ámbito del derecho civil también se reconoce la relación entre ambas figuras: el consentimiento es requisito necesario para la existencia de un contrato[1355], y para que ese consentimiento sea válido se requerirá previa información sobre los diferentes aspectos que caracterizan a dicho contrato[1356]. La jurisprudencia también ha resaltado la relación tan estrecha entre estos dos elementos[1357]. Al consentimiento informado se le reconocen, por lo tanto, dos acciones: la información y el consentimiento[1358].

En principio se trata de dos figuras independientes, con sentido y personalidad propia. En algunos supuestos puede darse el caso en que el consentimiento no sea necesario para el tratamiento de los datos de una persona determinada, pero sí la información. En el ámbito de la protección de datos el hecho de que en algún caso no se requiera consentimiento para tratar los datos de carácter personal no significa que no haya que informar. Hay que tener en cuenta que en esa información se revelan elementos tan importantes como los derechos que el titular de los datos puede ejercer con respecto a los mismos: acceso, rectificación, etc, sobre los que habrá que informar en la mayoría de los casos, incluso cuando haya alguna causa que exima al responsable del fichero de la obligación de recabar el consentimiento del titular. En estos supuestos el consentimiento y la información actúan de forma diferente. De esta circunstancia se

[1352] RODRÍGUEZ LÓPEZ, *La Autonomía...,* cit., 2004, p. 72; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 87.
[1353] Artículos 4.3 y 8.1 LBAP.
[1354] CANTERO MARTÍNEZ, *La Autonomía...*,cit., 2005, pp. 12 y 15; GUERRERO ZAPLANA, "El Consentimiento...", cit., 2003, pp. 102-103.
[1355] Artículo 1.261 CC.
[1356] DORAL, *El Contrato...*, cit., 1993, p. 71 y 94.
[1357] SAN 13 septiembre 2002, FJ 4: "no basta con la simple existencia del consentimiento, sino que este debe ser informado. (...) el tratamiento de datos no debe ser solamente legal, sino también leal, e implícito en dicho deber de lealtada se encuentra el de prestar una información adecuada al afectado o interesado, de forma que conozca el alcance real del consentimiento que presta"; STS, 13 julio 2007, FJ. 8: "La Ley orgánica 15/1999, de 13 de diciembre (...), de Protección de Datos de Carácter Personal, pone de manifiesto el carácter consustancial que el elemento de la información tiene con la prestación de consentimiento en relación con la disposición de los datos personales".
[1358] MÉJICA, y DÍEZ, *El Estatuto...*, cit., 2006, p. 37.

deduce la individualidad de ambos elementos. Sin embargo, en otros momentos esa autonomía puede ser cuestionada.

La falta de individualidad se puede deducir, por ejemplo, de la situación contraria a la expuesta. No puede imaginarse el caso en que se dé el consentimiento sin que exista información previa. Podría reconocerse este supuesto en el ejercicio del derecho a no saber, tan estudiado en el ámbito de la sanidad[1359] y perfectamente identificable también en el de la protección de datos. Si el derecho a la autodeterminación informativa supone el reconocimiento del control sobre los datos de cada uno, la libre disposición de esa información recogerá también la libertad para no saber lo que otra persona hace con ellos. Sin embargo, fuera de este supuesto específico, no puede concebirse el caso contrario en el que tiene que solicitarse la autorización mientras que la información queda excepcionada. El consentimiento no será válido si no es informado[1360]. No se puede consentir lo que no se conoce[1361]. Se podría llegar a la conclusión de que la información es en todo caso consustancial al ejercicio del consentimiento, por lo que no dejaría de ser redundante la utilización de la expresión consentimiento informado.

Cuando se habla del consentimiento informado se hace referencia, por lo tanto, a dos instituciones independientes que, sin embargo, tienen una relación o vinculación sustancial, hasta el punto de afirmar que ambos constituyen diferentes eslabones de la misma escalera. Los dos se fundamentan directamente en el mismo principio, el de autonomía, y se dirigen a la consecución del mismo fin, que no es otro que el de hacer efectiva la facultad del individuo de disponer libremente de sus datos. Cada uno tiene su momento, pues la información es previa al consentimiento, y el consentimiento supone la culminación del proceso de adopción de la decisión fundamentada que el titular va a adoptar sobre sus datos[1362]. No obstante, ambos responden al mismo fin inmediato: que la persona pueda tomar la decisión que estime más oportuna con relación a sus datos.

II. EL DERECHO A SER INFORMADO.

El derecho a ser informado, se puede adelantar desde ahora, constituye en términos generales la facultad de toda persona a conocer las características que van a rodear a los tratamientos de datos que le conciernen o afectan. La regulación que la LOPD realiza respecto de este derecho se recoge fundamentalmente en su artículo 5, que aquí se reproduce, a pesar de su extensión, debido a su importancia: "*1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a)De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; b)Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; c)De las consecuencias de la obtención de los datos o de la negativa a suministrarlo; d)De la posibilidad de ejercitar los derechos de acceso, rectificación,*

[1359] CANTERO MARTÍNEZ, *La Autonomía...*, cit., 2005, p. 12; MÉJICA y DÍEZ, *El Estatuto...,* cit., 2006, pp. 63-65.
[1360] RODRÍGUEZ LÓPEZ, *La Autonomía...,* cit., 2004, p. 95-96.
[1361] STS 31 de octubre de 2005, FJ 1; CANTERO MARTÍNEZ, *La Autonomía...,* cit., 2005, p. 15; DÍAZ REVORIO, "Derecho de la información…", cit., 2010, p. 435.
[1362] RODRÍGUEZ LÓPEZ, *La Autonomía...*, cit., 2004, p. 72.

cancelación y oposición; e)De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".

La Ley no recoge precepto alguno que regule el derecho a la información referido al tratamiento de datos de salud en el ámbito sanitario. Así como en lo que concierne al consentimiento se realizan previsiones concretas relativas a dicho supuesto, no ocurre lo mismo respecto al derecho a la información. Tampoco en la normativa sanitaria se recogen disposiciones concernientes a este punto. A falta de una regulación específica se entenderá que es aplicable al tratamiento de datos de salud en el ámbito sanitario el citado artículo 5, que afecta a la manipulación de todo tipo de datos. La aplicación de este régimen general a un sector con características tan particulares como el que aquí se trata planteará problemas. En todo caso, el régimen general que dispone la Ley para la regulación del derecho a la información deberá reinterpretarse cuando se trate de aplicar al ámbito sanitario. No hay que olvidar que los datos de salud son considerados por la LOPD datos sensibles. Sobre todo cuando haya que analizar las excepciones esta circunstancia hará que los límites tengan que interpretarse de manera más estricta o restrictiva.

II.1. Referencia a la relevancia del derecho a la información y su relación con otras facultades que componen el derecho a la autodeterminación informativa.

Como se ha dejado entrever en el apartado anterior, el derecho del titular de unos datos de carácter personal a ser informado sobre los aspectos que van a definir el tratamiento o la manipulación de los mismos se erige en facultad de extraordinaria relevancia para la salvaguarda del derecho a la autodeterminación informativa[1363]. Esta importancia ha quedado plasmada claramente en el ordenamiento jurídico. La ya derogada LORTAD, la actualmente vigente LOPD y la Directiva europea, reconocen este derecho como principio fundamental para la protección de datos.

La obligación de informar al titular de los datos sobre las características del tratamiento no deriva sólo de lo prescrito por las normas, sino que tiene su fundamento también en la buena fe. El responsable del fichero, para llevar a cabo una manipulación de datos acorde a la lealtad y honradez que requiere una vinculación como la que se genera entre este sujeto y el titular de los datos, necesariamente tendrá que cumplir con la obligación de informar de forma veraz y completa sobre las circunstancias que van a rodear el tratamiento de datos que pretende. En el ámbito interno la propia Ley recoge la necesidad de que los datos se recaben de forma leal[1364]. En el ámbito supranacional este llamamiento a la lealtad y a la buena fe para justificar el cumplimiento del deber de informar se pone de manifiesto tanto en la Directiva[1365] como en la Recomendación sobre la protección de datos médicos aprobada por el Consejo de Europa[1366]. Indudablemente, este requerimiento adquiere en el ámbito sanitario su máxima expresión, debido a las especiales características que presenta la relación de confianza que ha de haber entre el profesional sanitario y el paciente[1367]. Esta relación de confianza exige una actuación leal por parte de los sujetos participantes en ella.

La obligación de informar cuenta con una relevancia de gran alcance. Esta importancia viene dada por diferentes motivos. En primer lugar, el derecho a la información constituye el primer eslabón en el desarrollo de la relación que habrán de mantener el titular de unos datos de carácter personal y otro sujeto que tiene intención de manipular dichos datos. Erigiéndose en el punto de partida del citado vínculo, este derecho se convierte en la vía fundamental por la que el afectado por dicho tratamiento de datos toma conciencia real, para ese caso concreto, de su derecho a la autodeterminación informativa[1368]. Como se verá, habrá casos en que la información

[1363] MARTÍNEZ MARTÍNEZ, *Tecnologías de Información...,* cit., 2001, pp. 202-203; GUERRERO PICÓ, *El Impacto...*, cit., 2006, p. 251.
[1364] Artículo 4.7 LOPD: "*Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos*".
[1365] Considerando 38 Directiva 95/46/CE: *"Considerando que el tratamiento leal de datos supone que los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención".*
[1366] Artículo 4.1 R (97)5: "*Los datos médicos deben ser recogidos y procesados honrada y lealmente sólo para fines específicos".*
[1367] CANTERO MARTÍNEZ, *La Autonomía...*, cit., 2005, p. 12, hace referencia a la STS de 26 de septiembre de 2000 en la que se reconoce que "la información médica debe encuadrarse en el ámbito de la necesidad de actuar en forma acomodada a la buena fe que ha de presidir las relaciones contractuales, por estar inserta en el pacto médico-enfermo, y ello exige la previa información, que es iniciativa exclusiva del médico, como requisito previo para que el enfermo pueda emitir un consentimiento"; ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 94.
[1368] ARENAS RAMIRO, *El Derecho...*, cit., 2006, p. 97.

se exceptúe. También se encontrarán supuestos en que dicha información no se otorgue al titular en el momento mismo de la recogida, de forma que sea prorrogada y se dé en fechas posteriores a cuando los datos se recogen. No obstante, la mayoría de veces la importancia de esta figura viene determinada por ser el primer instrumento a través del cual se vincula en la práctica el titular de los datos a su derecho a la autodeterminación informativa.

En segundo lugar, desde el punto de vista puramente sustantivo la importancia del derecho a ser informado ha de ser analizada desde perspectivas diferentes. A) Hay que tomar en consideración este derecho desde su relación, ya apuntada, con el derecho a otorgar el consentimiento. Se ha dicho que la unión de estas dos figuras constituye un todo calificado como derecho a otorgar el consentimiento informado, que se erige en la principal facultad de control que tienen las personas sobre los datos que le conciernen. El derecho a ser informado está estrechamente vinculado al derecho a otorgar el consentimiento. Es, sin duda, requisito previo indispensable para poder ejercer la facultad de autorizar el posterior tratamiento de dichos datos[1369]. La propia jurisprudencia, atendiendo al articulado de la LOPD, ha resaltado el "carácter consustancial que el elemento de la información tiene con la prestación de consentimiento en relación con la disposición de los datos personales"[1370]. Para poder otorgar este consentimiento es necesario conocer los términos en los que este tratamiento se va a dar[1371]. Antes se ha dicho que la institución del consentimiento informado es reconocida también en la teoría del contrato. Precisamente en el ámbito del derecho civil se recoge una figura que refleja la especial relevancia de la información a la hora de otorgar el consentimiento. Se trata del "error"[1372]. La jurisprudencia en algún momento ha señalado que "el error es (...) el conocimiento falso de una cosa o de un hecho"[1373]. El consentimiento sobre algo que se desconoce o que se conoce de forma incorrecta, estará viciado siempre que se den los requisitos necesarios para contemplar dicho error[1374]. De la misma manera que el error a la hora de otorgar el consentimiento en la celebración de un contrato puede acarrear la nulidad del mismo, en el ámbito de la protección de

[1369] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 37.
[1370] STS 4 de abril del 2000, FJ 3.
[1371] Punto 106 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: "*It is obvious that such provisión of information is indispensable when the data subject is required to give his/her "informed" consent*".
[1372] Artículo 1.266 CC: "*Para que el error invalide el consentimiento deberá recaer sobre la sustancia de la cosa que fuere objeto del contrato, o sobre aquellas condiciones de la misma que principalmente hubiesen dado motivo a celebrarlo.*
El error sobre la persona sólo invalidará el contrato cuando la consideración a ella hubiera sido la causa principal del mismo.
El simple error de cuenta sólo dará lugar a su corrección".
[1373] SAP Salamanca, 5 de abril 2006, FJ. 3: ha recogido las palabras de CASTÁN para definir el error.
[1374] SAP Madrid, 5 de octubre 2006, FJ 6: "Para que concurra el error (...) el artículo 1.266 del Código Civil y la jurisprudencia exigen, a saber: recaer sobre la cosa que constituye su objeto o sobre aquellas condiciones que principalmente hubieran dado lugar a su celebración, de modo que se revele paladinamente su esencialidad; que no sea imputable a quien lo padece; un nexo causal entre el mismo y la finalidad que se pretendía en el negocio jurídico concertado, y que sea excusable, en el sentido de que sea inevitable, no habiendo podido ser evitado por el que lo padeció empleando una diligencia media o regular (...). Según la doctrina de esta Sala la excusabilidad ha de apreciarse valorando las circunstancias de toda índole que concurran en el caso, incluso las personales, tanto del que ha padecido el error, como las del otro contratante, pues la función básica del requisito es impedir que el ordenamiento proteja a quien ha padecido el error, cuando éste no mere esa protección por su conducta negligente; MÉJICA, y DÍEZ, *El Estatuto...,* cit., 2006, p. 51

datos la falta de información o la información errónea constituye un vicio insalvable en el consentimiento, pues supone autorizar lo desconocido[1375].

El derecho a la información, por lo tanto, aparece como elemento especialmente relevante en su vinculación con el derecho a otorgar el consentimiento[1376]. No obstante, la importancia del derecho a la información en esta relación se evidencia especialmente cuando la Ley no exige el consentimiento del titular de los datos para el tratamiento de los mismos.

En estos casos en que no se necesita la autorización del titular de los datos para su tratamiento, el derecho a ser informado constituye una garantía fundamental para la salvaguarda de la autodeterminación informativa. Supone la posibilidad de que el titular de los datos conozca quién, cuándo, cómo y para qué se van a tratar dichos datos, y sobre todo, cuáles son sus derechos con respecto a dicho tratamiento[1377]. La excepción al consentimiento no puede conllevar que el derecho a la autodeterminación informativa quede vacío de contenido. En los casos en que al titular de los datos se le niega la alternativa de autorizar o no el tratamiento de los mismos, la capacidad de controlar dichos datos se focaliza en el derecho a la información; la vía por la que el derecho a la autodeterminación informativa queda, se podría decir, vigente, es a través del ejercicio del derecho del afectado a ser informado sobre lo que se va a hacer con los datos que a él se refieren[1378]. La propia jurisprudencia ha reconocido en alguna ocasión de forma expresa la especial relevancia del derecho a ser informado cuando el consentimiento ha sido exceptuado. Una cosa es que el consentimiento sea limitado y otra que el titular tenga derecho a conocer lo que se hace con los mismos[1379]. Es lo que ocurre en el ámbito sanitario. En este sector como norma general se puede llegar a entender que el consentimiento queda exceptuado, en muchos casos, por las leyes. Siendo esto así, el derecho a ser informado se erige en la principal facultad para llevar a cabo el derecho a la autodeterminación informativa. A través de esta prerrogativa el titular de los datos conocerá lo que la Administración sanitaria va a realizar con los datos de cada uno y las facultades que le corresponden como afectado por ese tratamiento[1380].

B) La importancia del derecho a ser informado hay que vincularla a su relación con el derecho de consulta al registro correspondiente de protección de datos[1381] y el derecho de acceso[1382].

[1375] SEOANE RODRÍGUEZ, "De la Intimidad...", cit., 2002, p. 157.
[1376] DÍAZ REVORIO, "Derecho de la información…", cit., 2010, p. 435.
[1377] SÁNCHEZ CARAZO, en *Noticias Lopdate*, 2003; LÓPEZ AGÚNDEZ, "El Respaldo...", cit., 2003.
[1378] Resolución de la AEPD, R/00842/2007, 21 septiembre 2007, procedimiento AP/00037/2007.
[1379] STSJ de Andalucía, 18 de septiembre 2003, FJ. 2: "no puede confundirse la falta de consentimiento expreso para tratar un dato obtenido de una publicación oficial con la falta de conocimiento de que dicho dato, publicado oficialmente para un determinado fin de satisfacción de interés generales, acabe siendo tratado y cedido para otros fines comerciales. La Ley Orgánica protege el dato personal y su tratamiento y no puede mantenerse esta finalidad si el afectado por el dato desconoce su utilización. Entre otras cosas no puede solicitar su rectificación o actualización del dato".
[1380] SAN 15 de junio de 2001, FJ 3, reconoce expresamente la importancia del deber de informar en el ámbito sanitario, en atención a un supuesto en que se enjuicia el hecho de que en determinados centros se recaben datos de carácter personal relativos a donantes de sangre sin que se les informe sobre las características que van a rodear el tratamiento de esos datos.
[1381] Artículo 14 LOPD: "*Derecho de consulta al Registro General de Protección de Datos.- Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de*

Estas dos figuras y el derecho a ser informado constituyen un triángulo de facultades que componen, de alguna forma, un derecho a la información entendido en un sentido más amplio que el recogido en el artículo 5 de la LOPD.

El derecho a consultar el Registro General de la Agencia de Protección de Datos, ya sea el estatal o autonómico, constituye la posibilidad de todo ciudadano de conocer los ficheros existentes, sus responsables y sus finalidades. Por su parte, el derecho de acceso supone la posibilidad del interesado de conocer el contenido de los datos que se están tratando. Si a estas dos figuras se une la institución del derecho a la información en sentido estricto, que se erige en la facultad de conocer los parámetros que van a rodear el futuro tratamiento de los datos, se apreciará que, en última instancia, el titular de los datos tiene la posibilidad de acceder a una información completa sobre el tratamiento que se va a dar a sus datos en diferentes fases de dicho tratamiento: 1) siendo mero ciudadano, no interesado, con la posibilidad de acceder al registro correspondiente; 2) siendo titular de unos datos que se van a tratar, con el derecho a la información que en la recogida de datos asiste a todo afectado; y, 3) estando en marcha el tratamiento, con el derecho de acceso al contenido de los datos que se están tratando[1383].

En tercer lugar, la relevancia del derecho a la información hay que plantearla atendiendo estrictamente al contenido que ha de tener. En este sentido, el derecho se erige en imprescindible para conocer y ejercer los otros derechos de los que se es titular en el ejercicio de la autodeterminación informativa[1384], a saber: derecho de acceso, cancelación, rectificación y oposición fundamentalmente. En efecto, para llevar a cabo estos derechos es necesario tener conocimiento previo de su existencia y, precisamente, la información garantiza que el titular de los datos conozca dichas facultades y cómo ejercerlas. La jurisprudencia ha afirmado que el derecho a ser informado es "un derecho importantísimo porque es el que permite llevar a cabo el ejercicio de otros derechos"[1385]. De todo lo aquí expuesto fácilmente puede deducirse, pues, que se está ante un derecho de relevancia especial[1386].

II.2. Breve comentario sobre los sujetos participantes en el ejercicio del derecho a la información.

En relación a los sujetos que han de emitir y recibir la información a la que este apartado se refiere, no se plantean en este ámbito mayores problemas. No obstante, merece la pena realizar unos apuntes para comprender cuál es el alcance de esta figura.

---

tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita".

[1382] Artículo 15 LOPD: "*Derecho de acceso.-1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos*".

[1383] GONZÁLEZ MURUA, "Comentario a la STC...", cit., 1993, pp. 239-264.

[1384] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 186.

[1385] SAN, 15 de junio de 2001, FJ. 3; SÁNCHEZ CARAZO, *La Intimidad...*, cit., 2000, p. 107.

[1386] PIÑAR MAÑAS, "El País", 30 de diciembre de 2003: "el peor riesgo para nuestros datos es ignorar como se usan".

A) La LOPD no especifica quién ha de informar al titular de los datos sobre las características del tratamiento, pero, si se fija en el articulado de la misma y del Reglamento que la desarrolla, parece que será el responsable del fichero quien deberá llevar a cabo esta operación[1387]. Si bien esto es así, no ha de haber problema para admitir que el encargado del tratamiento también puede informar.

En el ámbito sanitario el responsable no es otro que el órgano de la correspondiente Administración sanitaria que tiene la capacidad de determinar la finalidad de dicho fichero al que se incorporarán los datos que se recaban[1388]. Es este órgano de la Administración quien ha de informar al paciente empleando los medios personales y tecnológicos de que dispone, mediante los médicos, los auxiliares, empleando medios informáticos, folletos, etc. Si este órgano responsable no lleva a cabo por sí mismo el tratamiento de los datos, sino que ha contratado los servicios de una empresa que desarrollará esta tarea en nombre y por cuenta de aquél, será el sujeto contratado, encargado del tratamiento, quien ejecutará la obligación de informar, en caso de que no lo haya hecho el responsable.

En lo que corresponde al sujeto concreto que ha de informar al titular hay que realizar un apunte. La LBAP[1389], al regular el deber de informar al paciente sobre su salud y el tratamiento médico a recibir, señala que ha de ser el médico el que ha de informarle[1390]. Puede tener sentido que en este caso la información la tenga que dar dicho profesional teniendo en cuenta cuál es su contenido. Se trata de transmitir al paciente cuál es su estado de salud, las características del tratamiento médico al que se va a someter, las alternativas existentes, etc. Será el médico la persona que con mayor precisión pueda explicar la citada información. Esto sucede cuando se trata de dar la información sanitaria. No parece que en el caso del derecho a la información reconocido en la LOPD tenga que ser el médico responsable obligatoriamente quien haya de llevar a cabo este ejercicio. La información que se integra en el derecho fundamental a la protección de datos no presenta la complejidad de la información sanitaria. Se trata de cuestiones más sencillas de comprender. Es por ello que esta información no requiere de la participación directa del médico[1391]. Así, puede entenderse que es posible que la Administración sanitaria emplee otros medios para llevar a cabo su obligación de informar.

B) Con respecto al sujeto que recibe la información cabe hacer un análisis algo más profundo. Como ya se ha dicho anteriormente, el derecho a la autodeterminación informativa se erige en un ejercicio de autonomía personal. Así, constituye prácticamente una tautología señalar que ha de ser el propio titular de los datos quien controlará los datos que le corresponden.

[1387] Artículo 5.1 LOPD, se cita al responsable; Artículo 18.2 RDLOPD, también se hace referencia al responsable.
[1388] APDM, *Guía de Protección…,* cit., 2004, p. 115: "En los ficheros de titularidad pública, el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia, teniendo capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza. Por ejemplo, la responsabilidad sobre el fichero de historias clínicas de un centro hospitalario corresponderá a la Gerencia del Hospital, mientras que el fichero de Datos de Personal de un centro corresponderá a la Dirección del mismo".
[1389] Artículo 4.3 LBAP: "*El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsable de informarle".*
[1390] CANTERO MARTÍNEZ, *La Autonomía...,* cit., 2005, p. 17.
[1391] BLAS ORBÁN, *El equilibrio...,* cit., 2006, pp. 155-157.

Teniendo en cuenta lo dicho, parece de sentido común afirmar que deberá ser dicho titular la persona a quien el responsable del fichero deberá informar y quien emitirá el consentimiento, cuando sea necesario, para que sus datos puedan ser tratados o manipulados. Así lo reconocen también las leyes expresamente[1392]. Esta circunstancia, sin embargo, no es obstáculo para admitir la posibilidad de que una persona nombre un representante que ejerza los derechos que le corresponden como titular de datos. Evidentemente, el ejercicio de los derechos de consentimiento e información en nombre de estas personas deberá hacerse con la autorización de éstas[1393]. Esta figura de la representación voluntaria se analizará más adelante cuando se estudien los derechos de acceso, cancelación, rectificación, oposición, etc.

Más allá de esta posibilidad de representación, hay que tener en cuenta que se pueden dar circunstancias en que la información al titular de los datos no será viable o recomendable. Se está hablando de la posibilidad de que el titular de los datos sea física o jurídicamente incapaz, o menor de edad.

En ningún caso puede pensarse que la minoría de edad o la incapacidad encubren una excepción al derecho a la información[1394]. En estas situaciones el deber de informar sigue vigente. Para estos supuestos hay que preguntarse si cabe el ejercicio del derecho por representación.

En algunos casos puede ocurrir que el interesado se encuentre en una situación en que es incapaz para ejercer el derecho, bien porque ha sido declarado como tal, o bien porque debido a circunstancias determinadas del momento no es posible llevar a cabo dicha información: casos de accidentes en que el paciente tiene un trastorno pasajero, por ejemplo. Para estos supuestos la Recomendación del Consejo de Europa sobre el tratamiento de datos médicos entiende que habrá que ver si el declarado como incapaz tiene o no facultad de comprender la información que se le va a dar. Si el profesional sanitario considera que el titular puede entender dicha información, no será necesario representante alguno[1395]. En caso contrario, la información habrá de darse a dicho representante o plantearse si cabe excepcionar o prorrogar este derecho.

Interesa analizar el caso en que el usuario o paciente es menor de edad, a pesar de que será una cuestión sobre la que se vuelva cuando se estudien los derechos de acceso, cancelación, rectificación, oposición, etc. Para estos supuestos es necesario plantearse la posibilidad del ejercicio del derecho por representación. La LOPD no aclara nada al respecto. Sin embargo, el nuevo RDLOPD sí pone la atención sobre este tema. Señala que deberá ser el propio responsable del fichero el que habrá de asegurarse de que concurre en el caso concreto el

[1392] Artículo 5.1 LOPD: "*Los interesados a los que se soliciten datos personales deberán ser informados (...)";* Artículo 6.1 LOPD: "*El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado (...)"*. En el mismo sentido se pronuncia la normativa referida a la autonomía del paciente: Artículo 4.2 LBAP: "*La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades (...)"*; Artículo 5.1, LBAP: "*El titular del derecho a la información es el paciente"*; Artículo 8.1 LBAP: "*Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario el afectado (...)"*.
[1393] SAN, 23 noviembre 2006.
[1394] Punto 123 Memoria Explicativa de la Recomendación R (97) 5 del Cosnejo de Europa.
[1395] Artículo 5.5 R (97) 5; MÉJICA y DÍEZ, *El Estatuto...,* cit., 2006, p. 55 y 62.

supuesto de minoría de edad y de que la actuación del representante de este menor es la correcta[1396]. Dispone también que en ningún caso se podrá recabar del menor de edad información sobre los demás miembros de la familia, más allá de los datos necesarios para que sus padres o tutores puedan llevar a cabo el ejercicio de su representación[1397].

El reglamento realiza una distinción atendiendo a la edad del menor. Respecto al consentimiento, los mayores de 14 años podrán consentir ellos mismos los tratamientos de los datos que les conciernen a no ser que una Ley disponga lo contrario. En el caso de los menores de esa edad, por el contrario, se requerirá el consentimiento de sus padres o de su tutor[1398]. En relación a la información el reglamento señala que ésta deberá prestarse a los menores de edad de forma que pueda ser comprendida sin mayor dificultad por los propios menores de edad[1399]. Se entiende aquí que podría emplearse el mismo criterio que para el consentimiento pues es difícil de imaginar que el menor de 14 años, como norma general, vaya a comprender los términos en que se le va a informar y las consecuencias jurídicas de lo que se le plantea[1400]. Sin embargo, a esta previsión podrían realizársele matices.

La cuestión de la representación ha sido tratada con mayor rigor en ámbitos diferentes al de la protección de datos, como es el puramente médico o asistencial. En general, las diferentes normas conceden soluciones distintas dependiendo del sector que se trate. Ciertamente, no es tarea fácil aportar una solución definitiva a una cuestión donde están en juego elementos que tanto tienen que ver con la bioética y la medicina[1401]. De ahí precisamente que las leyes que han entrado a regular esta materia no fijen un criterio unitario al respecto.

Lo cierto es que atendiendo a diferentes normas pueden llegar a encontrarse criterios incluso contrapuestos, otorgando plena capacidad de decisión al menor de edad o negándosela[1402]. En algunos supuestos las normas parecen prestar un amplio margen de actuación al menor de edad, valorando sobre todo su grado de madurez, más allá de que tenga una edad determinada[1403], mientras que en otros supuestos este margen de actuación se restringe, fijando límites en la

[1396] Artículo 13.4 RDLOPD.
[1397] Artículo 13.2 RDLOPD.
[1398] Artículo 13.1 RDLOPD.
[1399] Artículo 13.3 RDLOPD.
[1400] GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 229. "Mas, ¿un menor de 14 años es consciente de las repercusiones que puede tener el tratamiento de sus datos? ¿el menor va a entender los términos en que el art. 5 LOPD obliga al responsable a informarle? Esto sin contar con que el menor puede ser utilizado como cauta fuente de información sobre datos concernientes a sus familiares (...). La LOPD o su reglamento de desarrollo deberían ser más explícitos en lo que concierne a los menores".
[1401] BENAC URROZ, "La Problemática...", cit., 2004, p. 99.
[1402] SÁNCHEZ CARO y SÁNCHEZ-CARO, *El Médico...*, cit., 2001, pp. 201-208.
[1403] Artículo 162.1 CC: "*Los padres que ostentan la patria potestad tienen la representación legal de sus hijos menores no emancipados. Se exceptúan: 1. Los actos relativos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo".*
Artículo 5.1 LO 1/1996, 15 de enero, de Protección Jurídica del Menor: "*Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo".*
Artículo 3.1 LO 1/1982, 5 de mayo, de protección civil del derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen: "*El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil*".

capacidad de actuación atendiendo a una edad concreta[1404]. La importancia de la madurez se resalta también en el ámbito internacional en textos como el documento de trabajo sobre la protección de datos de carácter personal de los niños emitido por el Grupo de Trabajo del artículo 29 de la Directiva europea sobre protección de datos, en el que se presta especial atención a la madurez del menor para determinar hasta dónde alcanza su capacidad de obrar en relación al control que puede ejercer sobre la información que le concierne[1405]. En esta misma línea la doctrina que se ha dedicado a analizar esta cuestión señala la importancia que tiene que, incluso tratándose de un menor, le sea dada la información pertinente de manera comprensible al margen de que el consentimiento tenga que darlo su representante. Parece que se tiende a dar cada vez mayor importancia a lo que el menor de edad, dependiendo de su grado de madurez, pueda opinar al respecto de las cuestiones que le conciernen[1406]. Obviamente, deberá ser el propio profesional sanitario quien deba concluir si el menor es o no lo suficientemente maduro en cada caso[1407].

[1404] Artículo 9.3.c) LBAP: "*Se otorgará el consentimiento por representación en los siguientes supuestos: Cuando el paciente menor de edad no sea capaz intelectual ni emocionalmente de comprender el alcance de la intervención. En este caso, el consentimiento lo dará el representante legal del menor después de haber escuchado su opinión si tiene doce años cumplidos. Cuando se trate de menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, no cabe prestar el consentimiento por representación. Sin embargo, en caso de actuación de grave riesgo, según el criterio del facultativo, los padres serán informados y su opinión será tenida en cuenta para la toma de la decisión correspondiente".*
Artículo 9.4 LBAP: "*La interrupción voluntaria del embarazo, la práctica de ensayos clínicos y la práctica de técnicas de reproducción asistida se rigen por lo establecido con carácter general sobre la mayoría de edad y por las disposiciones especiales de aplicación".*
Artículo 11.1 LBAP: "*Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, (...)".*
Artículo 7.3 RD 223/2004, 6 de febrero, por el que se regulan los Ensayos Clínicos con Medicamentos: "*Cuando el sujeto del ensayo no sea una persona capaz para dar su consentimiento o no esté en condiciones de hacerlo, la decisión deberá adoptarse, teniendo en cuenta lo indicado en este artículo.*
Si el sujeto del ensayo es menor de edad:
Se obtendrá el consentimiento informado previo de los padres o del representante legal del menor; el consentimiento deberá reflejar la presunta voluntad del menor y podrá retirarse en cualquier momento sin perjuicio alguno para él. Cuando el menor tenga 12 o más años, deberá prestar además su consentimiento para participar en el ensayo.
El menor recibirá, de personal que cuente con experiencia en el trato con menores, una información sobre el ensayo, los riesgos y los beneficios adecuada a su capacidad de entendimiento.
El investigador aceptará el deseo explícito del menor de negarse a participar en el ensayo o de retirarse en cualquier momento, cuando éste sea capaz de formarse una opinión en función de la información recibida.
El promotor pondrá en conocimiento del Ministerio Fiscal las autorizaciones de los ensayos clínicos cuya población incluya a menores".
Artículo 7.2.d) Ley 21/2000, 29 de diciembre, sobre Derechos de Información concerniente a la Salud y la Autonomía del Paciente y a la Documentación Clínica: "*En el caso de menores, si éstos no son competentes, ni intelectual ni emocionalmente, para comprender el alcance de la intervención sobre su salud, el consentimiento debe darlo el representante del menor, después de haber escuchado, en todo caso, su opinión si es mayor de doce años. En los demás casos, y especialmente en casos de menores emancipados y adolescentes de más de dieciséis años, el menor debe dar personalmente su consentimiento.*
No obstante, en los supuestos legales de interrupción voluntaria del embarazo, de ensayos clínicos y de práctica de técnicas de reproducción humana asistida, se estará a lo establecido con carácter general por la legislación civil sobre mayoría de edad, y, si procede, la normativa específica que sea de aplicación".
[1405] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/2008, sobre la protección de datos de carácter personal de los niños, 18 de febrero de 2008, y Dictamen Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2009, sobre la protección de los datos personales de los niños, 11 de febrero de 2009.
[1406] LIZARRAGA BONELLI, Emilio, "La Información...", cit., 2004, pp. 266-267.
[1407]LIZARRAGA BONELLI, Emilio, "La Información...", cit., 2004, p. 269.

No se quiere en este momento analizar las diferentes teorías que pueden encontrarse sobre cuándo un individuo se convierte en maduro. Para lo que aquí interesa, basta con plantear una conclusión: si para cuestiones tan relevantes como las que pueden suponer aceptar un tratamiento médico determinado, la figura del menor de edad, incluso menor de 14 años, puede erigirse en individuo plenamente capaz para otorgar su consentimiento, parece justificado pensar que este menor puede tener capacidad, si se entiende que es lo suficientemente maduro, para recibir la información sobre los parámetros que rodearán al tratamiento de los datos que le conciernen. Se puede concluir, que tanto en el caso del incapaz como en el del menor de edad habrá de estarse al criterio del profesional sanitario para determinar si la información ha de darse al titular de los datos o/y a su representante.

A la hora de determinar el grado de participación que han de tener estos sujetos en el control a ejercer sobre los datos que les conciernen deberán tenerse en cuenta diferentes factores. Habrá que atender al grado de madurez general que presenta el titular de los datos. También deberá tomarse en consideración la incidencia que puede tener la manipulación de la información sobre los derechos del menor o supuesto incapaz. En este sentido, será necesario considerar la sensibilidad de los datos, pues no es el mismo el efecto que produce la manipulación de una información que puede considerarse sensible, al que produce el tratamiento de unos datos que no lo son. Y, fundamentalmente, habrá que tener en cuenta si la participación de un representante en el proceso de manipulación de datos puede llegar a vulnerar o afectar la intimidad del propio titular de los datos. No hay que pasar por alto que en estos supuestos, la representación puede suponer que los representantes tengan acceso a datos del titular que éste último no quiere que sean conocidos[1408]. Todos estos factores han de tomarse en consideración a la hora de determinar si un menor o supuesto incapaz puede prestar el consentimiento informado sobre una manipulación de sus datos.

II.3. El contenido del derecho a la información.

Atendiendo a la letra de la LOPD se tratarán ahora de analizar diferentes aspectos concernientes al contenido del derecho que ahora se comenta.

II.3.1. Sobre el momento en que se ha de llevar a cabo la información.

II.3.1.A. Distinción en la LOPD entre los casos en que los datos se recaban del propio titular y los supuestos en que se recogen de fuente distinta a éste.

El primer elemento a analizar en lo dispuesto en el artículo 5 de la LOPD es el relativo al momento en que ha de darse la información al titular de los datos. En principio el derecho a ser informado está vinculado al momento de la recogida de los datos de carácter personal[1409]. Sin

[1408] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/2008, sobre la protección de datos de carácter personal de los niños, 18 de febrero de 2008, y Dictamen Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2009, sobre la protección de los datos personales de los niños, 11 de febrero de 2009, en los que se reclama la necesidad de atender a diferentes factores a la hora de determinar el grado de madurez del menor y la posibilidad de su participación en el proceso de tratamiento de datos. PÉREZ LUÑO, "El consentimiento de los menores…", cit., 2010, pp. 483-485: se hace eco de la importancia del citado documento de trabajo.
[1409] Artículo 5.1 LOPD.

embargo, el artículo 5 reconoce en uno de sus apartados la posibilidad de que esta información se otorgue al titular más tarde de dicho momento de recogida[1410]. Se distinguen, por lo tanto, dos supuestos.

A) Normalmente los datos de carácter personal se recabarán directamente del propio titular. En estos casos es en el mismo momento en que se recogen los datos cuando se llevará a cabo la información al afectado. Esta regla tiene pleno sentido desde el punto de vista práctico. Cuando los datos son recogidos directamente del titular pueden darse dos supuestos: que se requiera su consentimiento o no.

En el primer caso parece obvio que la información tenga que darse en el momento de la recogida. Se ha dicho que sin información no puede haber consentimiento válido. Pues bien, si no hay tratamiento sin consentimiento, ni consentimiento sin información, es lógico exigir que la información sea el primer elemento en solicitar para llevar a cabo la manipulación de datos. El momento pertinente para ello será, evidentemente, el de la recogida de la información, pues es entonces cuando al titular se le pide que transmita sus datos y preste, después de ser informado, su consentimiento.

En el segundo supuesto, caso de que el consentimiento esté exceptuado pero la información sea requerida por la Ley para el tratamiento de los datos, cuando los datos se recogen del propio afectado, la información se dará también necesariamente en ese momento. Si los datos se recaban del propio titular, independientemente de que no se requiera su consentimiento, éste tendrá que ser informado en el mismo momento de la recogida. En caso de que los datos se recojan del propio titular, el ejercicio de la información en ese mismo momento será posible y exigible, pues prorrogar la información en este caso constituirá una afección innecesaria al derecho a la autodeterminación informativa.

Hay que tener en cuenta que cuando el consentimiento es exceptuado las facultades de control sobre los datos de cada uno se limitan en gran medida. En estos casos la información se convierte en un instrumento imprescindible para que el derecho a la autodeterminación informativa no se anule. Que este control, aunque limitado al ejercicio del derecho a la información, se lleve a cabo desde el momento de la recogida supone una garantía fundamental para el titular de los datos cuando esta persona tiene exceptuado el derecho a otorgar el consentimiento. El hecho de que esta facultad esté exceptuada, al igual que no limita el derecho a ser informado, tampoco niega la posibilidad de ejercer el derecho de acceso, rectificación y cancelación. Estos últimos derechos son esenciales, no ya por ser la expresión más clara de la autodeterminación informativa, como facultades positivas que son, sino porque constituyen un elemento indispensable para mantener la calidad de los datos. Los derechos de acceso, rectificación y cancelación hacen posible que el titular de la información pueda conocer los datos que se están tratando y ver si éstos se corresponden con la realidad presente, para, en caso contrario, cambiarlos y adecuarlos a la misma. Es conveniente que puedan ser ejercidos desde el momento en que tiene inicio el tratamiento, para que la calidad de los datos sea la adecuada. Hay que tener en cuenta que el ejercicio de estos derechos depende en gran medida de la previa

[1410] Artículo 5.4 LOPD.

información sobre la existencia y modo de ejercer de los mismos. Es necesario, pues, que la información sobre la facultad de acceso, cancelación y rectificación se lleve a cabo en el momento de la recogida, para que desde un inicio el titular de los datos tenga la posibilidad de ejercerlos.

B) Cuando los datos son recogidos directamente de su titular, por lo tanto, la información sobre las características que rodearán al tratamiento de dichos datos se deberá dar en el momento de su recogida. Cosa distinta ocurre cuando no han sido recogidos directamente de su titular. Esto sucede cuando se recaban de una tercera persona o de fuentes accesibles al público. En estos supuestos la Ley estatal exige que el interesado sea informado dentro de los *"tres meses siguientes al momento del registro de los datos"*[1411]. Para estos casos no se requiere que la información se dé en el momento de la recogida de los datos, sino que puede retrasarse en el tiempo hasta un plazo máximo de tres meses. La Ley no establece en base a qué criterio se determinará el momento en que ha de darse la información dentro de estos tres meses, ni en qué bien jurídico se fundamentará la justificación de esta prórroga. Realmente, la regulación de la LOPD sobre este aspecto es confusa y exige una reflexión[1412].

En primer lugar, hay que determinar a qué supuestos es aplicable este precepto. De la redacción de la Ley se deduce que los datos pueden ser recabados en un momento determinado sin que en ese instante se le otorgue información alguna al titular. La recogida puede llevarse a cabo sin que se dé la debida información al titular de los datos. No obstante, más allá de la recogida ¿pueden ser manipulados o utilizados, los datos, sin que haya sido llevada a cabo dicha información? Parece que este último supuesto tiene cabida en la LOPD. Efectivamente, la Ley no dice expresamente si en ese plazo de tres meses pueden tratarse los datos o no. No obstante, se puede entender que ésta es la posibilidad que prevé la norma. La fijación de un plazo máximo es fruto de la preocupación de que los datos puedan manipularse durante un plazo mayor al señalado. Esa preocupación no puede derivar de otro hecho que no sea la posibilidad de que los datos puedan ser tratados sin que se haya llevado a cabo la información. La disposición de la LOPD que se estudia, por lo tanto, recoge el caso en que los datos recabados de persona distinta al titular de los mismos comienzan a ser manipulados sin haberle informado a éste oportunamente de las características principales que rodean a dicho tratamiento[1413].

En segundo lugar, cabe preguntarse si la prórroga en la información puede constituir una prórroga en el consentimiento. Esta cuestión llevará a la conclusión de que en este plazo en el que queda prorrogado el ejercicio del derecho a la información no podrán tratarse datos en los casos en que el consentimiento del titular sea requerido.

[1411] Artículo 5.4 LOPD.
[1412] La normativa autonómica no aclara en ningún sentido la regulación estatal. La norma vasca no recoge plazo alguno para el ejercicio de la información cuando los datos son recogidos de fuente ajena al titular de los datos y la Ley madrileña realiza una remisión a la norma estatal. Artículo 6, Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos*;* Artículo 6, Ley 8/2001, 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.
[1413] APARICIO SALOM, *Estudio sobre…,* cit., 2009, p. 132.

Como se ha apuntado, el consentimiento necesita de la información para ser válido. Si la información ha sido prorrogada es evidente que el tratamiento no podrá tener inicio con el correspondiente consentimiento informado. Si un tratamiento requiere el consentimiento para ser llevado a cabo y éste, a su vez, exige de la información, no puede existir supuesto en que quepa un tratamiento sin información pero con consentimiento. El consentimiento no puede darse si no hay previamente una información. Así pues, no cabe el caso en que un tratamiento tenga inicio con consentimiento pero sin información. Esta afirmación lleva a la conclusión de que el artículo 5.4 de la LOPD está pensado para los supuestos en que el consentimiento del titular está excepcionado por alguna de las causas que más adelante se verán. El único supuesto en que el tratamiento de los datos puede tener inicio, sin que se haya dado la información correspondiente al titular de los datos, es ese en que el consentimiento del titular se encuentra exceptuado.

Se podría interpretar que la causa que justifica que un tratamiento de los datos comience sin que se haya otorgado al titular de dichos datos la información pertinente sobre las características que van a rodear al tratamiento justifica también una prórroga en el ejercicio del consentimiento, de tal forma que en ese plazo se podrían tratar los datos sin que existiese la autorización oportuna del afectado. Esta posición no es aceptable. La prórroga para el ejercicio del derecho a la información no puede justificar por sí misma la prórroga para el derecho a otorgar el consentimiento. Si el legislador hubiera querido reconocer un supuesto en que, cuando los datos son recabados por persona ajena al titular, el tratamiento puede llevarse a cabo sin que exista consentimiento informado cuando éste es necesario, debería reconocerlo de forma expresa y justificarlo basándose en la protección de algún bien jurídico suficiente. El ordenamiento no recoge supuesto alguno en que un tratamiento que requiera el consentimiento del titular pueda tener inicio sin que dicho consentimiento se haya recabado, es decir, no se recoge caso alguno en que el consentimiento pueda ser prorrogado. En el artículo que ahora se comenta, y que reconoce una prórroga al ejercicio del derecho a la información, no se recoge una prórroga al consentimiento.

El caso recogido en el comentado artículo de la norma estatal es pues el siguiente. Se trata del supuesto en que los datos son recogidos por una persona ajena a su titular, en que el derecho a otorgar el consentimiento está excepcionado y la información puede ser otorgada con posterioridad a la recogida de los datos. No parece que pueda haber más supuestos del que se acaba de plantear.

La prórroga de la información tendrá que estar justificada. Iniciar un tratamiento de datos de carácter personal sin haber informado al titular de los datos supone una limitación del derecho a la autodeterminación informativa. La Ley no establece en base a qué bien jurídico se justifica esta prórroga. No obstante, y teniendo en cuenta los supuestos en que se puede aplicar el artículo ahora comentado, es posible interpretar que esta limitación sólo podrá estar fundamentada, precisamente, en esos motivos que a su vez excepcionan el consentimiento del titular. La prórroga en la información es aplicable solamente a los casos en que se exceptúa el consentimiento. Pues bien, la causa que justifica la excepción al consentimiento no excepciona a su vez el derecho a recibir la información, pero sí puede justificar su prórroga siempre que ésta sea necesaria.

Por último, hay que analizar si es ajustada a Derecho o no la fijación del plazo de tres meses que establece la Ley estatal para llevar a cabo la información. Para ello la Ley ha de ser comparada con las normas aplicadas en el ámbito supranacional. La Directiva reguladora de la protección de datos de carácter personal fija que en los supuestos en que los datos no hayan sido recabados de los afectados, éstos deberán ser informados *"desde el momento del registro de los datos"* o *"en caso de que se piense comunicar datos a un tercero, a más tardar en el momento de la primera comunicación"*[1414]. Por su parte, desde el Consejo de Europa se recoge la obligación de informar *"tan pronto como sea posible"*[1415]. En relación a la prórroga que plantean todas estas normas para llevar a cabo la información pueden plantearse diferentes cuestiones.

La norma estatal señala que el plazo de tres meses se computará desde el registro de los datos. Cabe preguntarse si la expresión "el registro de los datos" se refiere a la recogida de los datos y su incorporación al fichero o al registro del fichero en el Registro de ficheros de la Agencia de Protección de Datos que corresponda. Se entiende aquí que el plazo de tres meses ha de computarse desde que se incorporan los datos al fichero oportuno, es decir, desde la recogida de los datos de fuente distinta al afectado. Hay que tener en cuenta que cuando los datos son recabados del propio titular la referencia temporal para llevar a cabo la información es el momento de la recogida. Así, tiene sentido que para tomar una referencia para computar los tres meses correspondientes se emplee también el momento de la recogida de los datos. Se trata de una interpretación favorable a los intereses del titular de los datos, pues, un criterio distinto al planteado podría retrasar la información más allá de los tres meses señalados por la Ley.

En cuanto a lo dispuesto en la Directiva europea hay que señalar que su redacción es algo confusa. En principio, parece que pueden distinguirse dos supuestos en los que cabe una prórroga a la información: el que se refiere a los casos en que no se prevé una cesión de los datos recogidos, y el supuesto en que se da una cesión de dichos datos.

Para estos últimos casos la regla a seguir aparece lo suficientemente definida. La información se deberá dar como muy tarde en el momento de la primera comunicación. Se permite por lo tanto que haya un período desde la recogida de los datos sin que se haya dado información al titular de los datos. No obstante, este período de prórroga no podrá extenderse más allá de la primera comunicación. La crítica a este planteamiento es inevitable. Señalar un límite de tiempo para llevar a cabo la información como puede ser la realización de la primera comunicación tiene un riesgo de envergadura: que la primera comunicación se retrase excesivamente en el tiempo.

Para el primero de los casos, cuando no hay cesión de datos prevista en el tratamiento, la regla no aparece muy definida en la norma europea. Dispone que la información se dará desde el momento del registro de los datos. Podría entenderse que la información ha de otorgarse en el momento en que se incluyen los datos en el fichero. Hay que tener en cuenta que en la versión inglesa de la Directiva se emplea la expresión "*at the time"*, "en el momento", lo cual podría apoyar la tesis de que la información tiene que darse en el momento en que los datos se registren. El empleo de la preposición "desde" genera ciertas dudas y da a entender que la

[1414] Artículo 11.1 Directiva 95/46/CE.
[1415] Artículo 5.2 R (97) 5.

información podrá darse en cualquier momento a partir de que se registren los datos. Lógicamente, no puede admitirse la inexistencia de un límite de tiempo para el ejercicio de la información. De una interpretación conjunta de la regulación dada a ambos supuestos puede deducirse que la Directiva aboga por que la información se dé lo antes posible. Si para los casos en que una cesión está prevista se permite que la información se prorrogue hasta que la primera comunicación se dé, es difícil entender que en los casos en que no está prevista dicha cesión la información tenga que darse en el mismo momento en que los datos son incorporados al fichero. No parece que tenga sentido que para un caso se prevea la posibilidad de prórroga en la información y para el otro no. Ahora bien, lo que tampoco puede interpretarse es que dicha prórroga no tenga límite alguno.

De una lectura global del artículo 11 de la norma europea se intuye que la intención del legislador europeo es que se informe cuanto antes al titular de los datos. Esta misma interpretación parece recogerse en la Recomendación del Consejo de Europa cuando señala que la información deberá darse tan pronto sea posible.

Ciertamente, esta última interpretación es la más coherente con el contenido del derecho a la autodeterminación informativa. La idea de que unos datos de carácter personal puedan ser tratados sin que se haya dado la información oportuna al titular de los datos, no habiendo causa justificativa para ello, no se puede mantener desde una postura garantizadora del núcleo de este derecho fundamental. El tratamiento sin mediar la previa información constituye una situación excepcional y, por eso, no puede mantenerse más allá del tiempo estrictamente necesario. De lo dispuesto en la normativa supranacional se deduce la exigencia de que, en los casos en que la información se obtenga de una fuente ajena al propio afectado, éste sea informado, en todo caso, lo antes posible.

Frente a esta regulación recogida en la normativa internacional, el plazo de tres meses que otorga la LOPD, sin mayor precisión, al responsable del fichero para hacer efectiva la información carece absolutamente de fundamento[1416]. No parece que la transposición de la Directiva al ámbito interno se haya llevado a cabo de manera adecuada, sin embargo, cabe realizar una interpretación de la LOPD acorde a las normas internacionales. La posibilidad de que puedan transcurrir tres meses en los que el titular de los datos no tenga conocimiento alguno sobre el tratamiento que de dichos datos se está realizando, es rechazable desde todos los puntos de vista, por lo que habrá que interpretar el precepto de acuerdo con la Directiva y con la Recomendación que se han citado, de forma especialmente restrictiva[1417]: deberá informarse al titular de los datos lo antes posible, y a más tardar en el plazo de tres meses.

[1416] GARCÍA-BERRIO HERNÁNDEZ, *Informática y Libertades...*, cit., 2003, p. 194; COLLADO GARCÍA-LAJARA, *Protección de Datos...*, cit., 2000, p. 18; HERRÁN ORTIZ, *El Derecho...,* cit., 2002, pp. 217-218.

[1417] En el primer Informe de la Comisión Europea sobre la Transposición de la Directiva 95/46/CE, de 15 de mayo de 2003, COM (2003) 265 final, la citada institución europea considera que el plazo de tres meses que la normativa española otorga al responsable del fichero para llevar a cabo la información, supone una interpretación demasiado laxa del artículo 11.1 de la Directiva 95/46/CE.

II.3.1.B. Aplicación de esta regulación en el ámbito sanitario.

Lo comentado hasta ahora en relación al momento en que ha de darse la información al titular de los datos ha de tratar de aplicarse en el ámbito sanitario, teniendo en cuenta las particularidades que presenta la manipulación de datos de carácter personal en este sector. Fundamentalmente, hay que tomar en consideración que la casuística es muy variada y que dependiendo de las circunstancias que rodean a cada caso la información se dará de una manera, de otra, o no se dará como se verá más adelante.

La mayoría de las veces los datos se recaban en la práctica sanitaria de los propios afectados, bien vía oral en las consultas o bien a través de la realización de intervenciones en el cuerpo de los pacientes. Como se ha visto, la Ley exige que cuando los datos son recabados del titular la información sobre las características del tratamiento se transmita en ese mismo momento. En el campo sanitario hay situaciones en que esto no será posible. La recogida de datos del propio titular puede producirse en circunstancias muy diversas y no siempre podrá llevarse a cabo la información en el momento mismo de la recogida. Lógicamente, cuando una persona acude a una consulta o va a ser intervenido voluntariamente no hay problema para que se cumpla con el requisito citado. Sin embargo, pueden darse casos en que, debido a la urgencia de la situación, se recaben datos del propio paciente sin que se pueda cumplir con la obligación de informar al titular de los datos o a su representante. En estas situaciones, bien por la necesidad de actuar con extrema celeridad, o bien por la situación en que se encuentra el paciente, la información resulta imposible. En estos supuestos, a pesar de que la fuente es el propio titular, cabe plantearse la posibilidad de aplicar una prórroga al ejercicio de la información, si esta es exigible, hasta que la misma pueda llevarse a cabo.

En otros supuestos los datos no se recogen del propio titular sino que son recabados de terceras personas: de familiares o allegados, de otras administraciones u otros órganos responsables, etc. El caso de las cesiones es el más representativo. En ocasiones, cuando los datos son recabados por fuentes distintas a su titular el deber de informar puede cumplirse en el momento de la recogida. Sin embargo, en determinadas circunstancias el ejercicio de esta obligación puede plantear problemas prácticos de envergadura: gran cantidad de sujetos a los que se debe informar, urgencia en la realización de una operación que imposibilita la información inmediata, dificultades a la hora de localizar a los titulares de los datos, etc. Piénsese en la obligación de informar a todos los titulares de datos que son tratados, por ejemplo, en determinadas investigaciones que manejan unas grandes bases de datos. La información inmediata resultaría poco menos que materialmente imposible. Estas contingencias pueden llevar a que la información en el momento de la recogida sea difícil de realizar. Es aquí cuando cabría aplicar la comentada prórroga prevista en el artículo 5.4 LOPD.

Como se acaba de ver, las diferentes posibilidades que prevé la LOPD tienen su aplicación en el ámbito sanitario, debido a que los datos se recogen indistintamente tanto del propio titular como de terceras fuentes. No obstante, esta aproximación al ejercicio de la información en el ámbito sanitario no puede esconder el hecho de que en este sector la aplicación de la letra de la Ley es más compleja de lo que en un inicio pudiera parecer.

La Ley fija unos parámetros generales, más o menos acertados, sobre el momento de llevar a cabo la información al afectado. La aplicación del esquema dispuesto por la norma a las circunstancias concretas que se dan en el ámbito de la sanidad es problemática. Las particularidades que presenta este sector exigen que haya una regla más flexible para el efectivo ejercicio de la información en el tratamiento de los datos sanitarios.

Como punto de partida parece exigible que en el inicio de la relación entre la Administración sanitaria y el usuario se dé una información general sobre cómo se van a emplear sus datos. Esta información se podrá llevar a cabo a través de medios que posibiliten una perpetuación de la misma: carteles, folletos, boletines, información a cada paciente cuando se le entrega la tarjeta sanitaria, etc. Se trata de información general válida para todo usuario del sistema sanitario, sobre posibles usos de los datos, derechos de los interesados en relación a dichos datos, quién es el responsable de los ficheros y cómo contactar con él, etc. Más allá de esta información, cada acto concreto que se lleve a cabo en la práctica sanitaria, operaciones, análisis médicos por distintos especialistas, investigaciones, cesiones internas de la historia clínica, etc., requiere de un análisis particularizado. Evidentemente, una Ley orgánica como la LOPD no puede entrar a fijar soluciones para cada caso particular.

Para el ejercicio de la información, en principio, habrá que seguir lo dispuesto por la Ley, distinguiendo los supuestos en que los datos son recabados del propio titular o no. No obstante, vistas las dificultades que en algunos casos las características del ejercicio de la sanidad presentan, más allá de estas reglas generales que aporta la Ley, habrá de estar al principio más amplio de que la información individualizada concerniente a la manipulación de datos en cada acto sanitario concreto se deberá dar, si es necesaria, cuando sea posible.

Cada acto sanitario plantea problemas concretos y el profesional sanitario no puede cuestionarse en cada momento cuándo ha de informar al titular. Como se ha adelantado, no todo acto sanitario que implica un tratamiento de datos exige que haya una información al titular sobre los parámetros que van a rodear a dicha manipulación. Habrá que valorar en qué medida cada uno de estos actos constituye una nueva manipulación de datos que afecta al derecho a la autodeterminación informativa, de tal manera que requiera la información exigida del artículo 5 LOPD.

Cuando los datos son recabados del propio titular la información se le deberá trasladar en el instante mismo de la recogida. Sin embargo, como se ha apuntado, pueden darse casos especiales en que puede estar justificado el retraso en la información debido a la particularidad de las circunstancias: caso de alguna urgencia, por ejemplo[1418]. Es lo que se apunta también por parte de las agencias de protección de datos en relación a servicios, por ejemplo, de teleasistencia en que las circunstancias de gravedad de determinadas situaciones harán que la información se preste por vías alternativas[1419].

[1418] ARENAS RAMIRO, *El Derecho...,* cit., 2006, p. 98, expone, haciendo referencia a otros ámbitos de la realidad, algún supuesto que justifica la posibilidad de prórroga para llevar a cabo la información cuando los datos son recabados del propio titular.
[1419] Dictamen AVPD CN09-021, 24 septiembre de 2009.

Cuando los datos se recogen de terceras fuentes la información al titular puede prorrogarse hasta un plazo máximo de tres meses. La recogida de datos de fuente distinta al titular se da principalmente a través de cesiones datos. No obstante, dentro de las comunicaciones pueden distinguirse diversos supuestos. Son distintos, por ejemplo, el caso de una enfermedad mental en la que personas cercanas al paciente transmiten información sobre el comportamiento del paciente titular de los datos y el supuesto en que se remiten unos datos de un centro sanitario a otra entidad para que lleven a cabo una investigación[1420].

En el primer caso, la información aportada por terceras personas se complementa con información dada por el propio paciente en un único fichero. En estos supuestos, normalmente, la obligación de informar ya ha sido ejecutada con anterioridad cuando el paciente inició el tratamiento médico, por lo que no es necesario que se lleve a cabo otra vez la misma información por el mero hecho de que una tercera persona haya aportado nuevos datos. Además, el paciente, en el ejercicio de su derecho de acceso que más adelante se analizará, puede tener, salvo limitación justificada, conocimiento de los datos que se están manipulando sobre su estado de salud, incluso de los aportados por terceras personas.

Algo parecido ocurre cuando se produce una mera transmisión de datos de salud para llevar a cabo un acto concreto como podría ser, por ejemplo, dispensar una receta en una farmacia aplicando la receta electrónica, sin que esa comunicación de datos conlleve una nueva manipulación sobre la que no ha sido informado el titular. La dispensa del medicamento se trata de un acto puntual que no requiere, según se entiende aquí, del ejercicio de una información individualizada completa. El hecho de que el médico transmita unos datos concretos a un farmacéutico para que este último pueda dispensar un medicamento, con unas mayores garantías, no puede obligar al farmacéutico a informar al paciente sobre todo lo que va a rodear ese acto puntual, pues la información simplemente se limitaría a la mera existencia de dicho trámite. Lo contrario llevaría a una excesiva burocratización del sistema, pues supondría que en cada acto de dispensa tuviera que informar sobre las características de un tratamiento que, en la mayoría de los casos, se va a agotar con su realización. Otra cosa sería que el farmacéutico archivase y conservase esos datos para manipularlos posteriormente con diversos fines, situación que, como se verá más adelante, en la práctica sucede[1421].

En estos dos supuestos, los datos son recabados de fuente distinta al titular, sin embargo, las transmisiones de datos no llevan a la creación de nuevos ficheros. El tratamiento al que conducen estas comunicaciones consiste en un acto puntual que exige, como mucho, una información limitada a la existencia misma de la transmisión de datos que se ha dado entre distintos sujetos.

Cosa distinta sucede, en la segunda situación, cuando de la cesión de datos nace un nuevo tratamiento. Cuando la comunicación lleva a una nueva manipulación con nuevas finalidades

[1420] PAÉZ MAÑA, *La Protección...,* cit: afirma que "nada impide al personal sanitario, dialogar en forma distendida, con aquellas personas que puedan aportar información relevante sobre la causa de la prestación asistencial (pacientes, familiares, allegados, etc.) sino todo lo contrario".

[1421] RD 1718/2010, 17 de diciembre, sobre Receta Médica y Órdenes de Dispensación, donde se reconocen diversos casos en que se obliga a los profesionales farmacéuticos a conservar información y transmitirla con distintos fines.

será necesario que se respeten todas las garantías posibles. Piénsese en el supuesto de una transmisión de datos de un centro sanitario a otra entidad para llevar a cabo, por ejemplo, estudios epidemiológicos. Este caso se da en la práctica en numerosas ocasiones[1422]. Los datos son recogidos por el segundo órgano de fuente distinta al titular y serán empleados con una nueva finalidad. En estos supuestos el derecho a ser informado debe quedar salvaguardado en toda su extensión. La información ha de ser completa. El problema reside en determinar cómo ha de garantizarse su cumplimiento. En estos supuestos habrá que ver si se puede aplicar alguna excepción al derecho a la información. En caso de que no sea así, la información deberá llevarse a cabo, siempre, lo antes posible y a más tardar en el plazo máximo de tres meses.

II.3.2. Sobre la necesidad de que se informe de forma expresa, precisa e inequívoca.

Desde un punto de vista formal, es de interés analizar la manera en que se ha de llevar a cabo el deber de informar por parte del responsable del fichero.

II.3.2.A. La prohibición en la LOPD de que la información sea ambigua, confusa o genérica.

La norma estatal exige que se informe de "*modo expreso, preciso e inequívoco"*[1423]. Asimismo, el RDLOPD requería que la información se ejerciera de tal modo que permitiera comprobar que se ha llevado a cabo[1424]. La Directiva europea, por su parte, reclama que la información sea "*precisa y completa*"[1425]. De una primera lectura conjunta de estos preceptos se deduce que se exige cierto rigor en la forma a la hora de que el responsable del fichero lleve a cabo la información.

La información tiene que darse al titular de los datos de forma expresa. Por lo tanto, tiene que ir dirigida al afectado sin que éste tenga que llevar a cabo un ejercicio de deducción[1426]. En segundo lugar, la información no puede darse de manera ambigua, sino que tiene que ser precisa, exacta, referida a las cuestiones concretas que exige el ordenamiento. Y por último, no puede dar lugar a dudas o equívocos[1427], de manera que ha de ser clara. Además, como dispone la Directiva, la información ha de ser completa, referida a todos los aspectos que van a rodear al tratamiento de los datos. Este último requisito queda concretado en la Ley estatal al apuntar expresamente el contenido sobre el que se ha de informar necesariamente.

De lo que se acaba de exponer queda claro que no hay lugar para las informaciones genéricas o ambiguas. Y lo que sin duda es más subrayable, la información ha de darse de manera que no haya duda de que el interesado la ha recibido. El recurso a la letra pequeña no es

[1422] Orden de 18 de diciembre de 2000, por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH), en la que se prevén las siguientes cesiones de los datos sanitarios que se recaben en cumplimiento de la norma: "*Organización Mundial de la Salud/Centro Europeo para la Vigilancia Epidemiológica del VIH (datos anónimos), Comunidades Autónomas, Organismos de Investigación,*"
[1423] Artículo 5.1 LOPD.
[1424] Artículo 18 RDLOPD, que ha sido invalidado por la STS 15 de julio de 2010.
[1425] Considerando 38 Directiva 95/46/CE.
[1426] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 38.
[1427] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 38.

válido[1428]. Parece clara la voluntad del legislador de que se garantice siempre que el titular de los datos tenga conocimiento de todos los aspectos que van a rodear el tratamiento de la información que le concierne. En este sentido, en más de una ocasión la AEPD, en relación a diferentes ámbitos de la realidad, ha realizado recomendaciones sobre la necesidad de que se adopten medidas que garanticen el cumplimiento de este requisito[1429].

Esta rigurosidad en la forma que se exige a la hora de informar al titular de los datos se refuerza cuando para la recogida de dichos datos se emplean cuestionarios u otros impresos. Para estos supuestos la LOPD exige que la información figure "*en forma claramente legible*"[1430]. El calificativo legible hace referencia a lo que se puede leer[1431]. Parece que en estos casos se requiere que la información se fije de forma escrita, ya que para que ésta pueda ser legible es necesario en primer lugar que esté escrita. Así lo han reconocido también las resoluciones de la AEPD[1432]. De alguna manera, se aprovecha el hecho de que la recogida de datos se lleva a cabo a través de un documento, sea en el formato que sea, para establecer mayores garantías de que el titular de los datos accede a la información que la Ley exige que se le dé[1433].

Si para estos casos la Ley exige que la información se dé de manera escrita, puede plantearse que para los demás supuestos dicha información no tenga que transmitirse de esta manera. Cuando la recogida de datos no se realice con cuestionarios bastará con que sea oral[1434]. Para los casos en que quiere que la información conste de forma escrita el legislador lo indica expresamente, por lo que se entenderá que en los supuestos en que no lleva a cabo ninguna indicación no exige que la información se refleje de esta manera. Así lo ha indicado también la jurisprudencia[1435]. El problema que esta regulación plantea es, obviamente, la dificultad de probar que dicha información se ha llevado a cabo cuando ésta no se ha producido por escrito. El Reglamento que desarrolla la Ley exigía que el deber de informar se llevara a cabo a través de un medio que permitiera acreditar su cumplimiento[1436]. Esta previsión, sin embargo, ha sido anulada recientemente por los tribunales al considerar que atenta contra la citada libertad de forma por la que aboga la Ley[1437]. Evidentemente, en la medida en que el RDLOPD exigía que

[1428] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 38.
[1429] Recomendación de la AEPD en relación a la actividad de Selección de Personal a traves de Internet, 17 de noviembre 2005: hablando de la necesidad de informar, cuando se refiere a los servicios que se prestan en las páginas web se recomienda que "A pesar de que se pueda incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un "click", permita obtener la citada información, se considera más apropiado propiciar la lectura de dicha información de modo ineludible (y no optativa) dentro del flujo de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos".
[1430] Artículo 5.2, LOPD.
[1431] http://www.rae.es/
[1432] Resolución de la AEPD, R/00017/2008, 15 enero 2008, procedimiento PS/00231/2007.
[1433] Resolución de la AEPD, R/00842/2007, 21 septiembre 2007, procedimiento AP/00037/2007.
[1434] ORTÍ VALLEJO, *Derecho a la Intimidad...*, cit., 1994, p. 139.
[1435] STS 15 de julio de 2010, FJ 9: "debe considerarse que el legislador ha optado por al libertad de forma".
[1436] Artículo 18 RDLOPD: "*1. El deber de información al que se refiere el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado.*
2.El responsable del fichero o tratamiento deberá conservar el soporte en el que conste el cumplimiento del deber de informar. Para el almacenamiento de los soportes, el responsable del fichero o tratamiento podrá utilizar medios informáticos o telemáticos. En particular podrá proceder al escaneado de la documentación en soporte papel, siempre y cuando se garantice que en dicha automatización no ha medado alteración alguna de los soportes originales".
[1437] STS 15 de julio de 2010, FJ 6.

la información se diera de manera que quedara probada, limitaba la forma a emplear a la hora de informar al titular de los datos. A pesar de la consideración de los tribunales, se entiende aquí que lo más acertado sigue siendo que la información se lleve a cabo mediante un escrito, y si la información se emite vía oral es aconsejable el empleo de medios como grabadoras, que permitan su prueba. Lo contrario podría llevar al responsable o encargado a tener que buscar indicios que demuestren el cumplimiento de la obligación señalada. Es conocida la gran cantidad de sanciones impuestas por la agencia por el incumplimiento del deber de informar. Siendo esto así, resulta recomendable que conste por escrito que se ha dado la información de forma adecuada, más en ámbitos como el sanitario, donde las denuncias por falta de información sobre el tratamiento médico que se va a dar al paciente están a la orden del día.

El ejercicio del derecho a la información exige, por lo tanto, el cumplimiento de una serie de requisitos en garantía de que al titular de los datos le queden absolutamente claros los parámetros en los que se va a desarrollar el tratamiento de sus datos. Este requerimiento puede plantear numerosos problemas cuando se trata de llevar a la práctica. En la realidad se pueden dar innumerables casos en que informar al titular de los datos de la forma en que exige la Ley no sea fácil. Esto sucede cuando en la manipulación de datos que se va a llevar a cabo confluyen diferentes bienes jurídicos de relevancia equiparable que pueden llegar a chocar. Si el ejercicio del derecho a ser informado obstaculiza la efectiva realización de otro bien jurídico, habrá que atender a las particularidades de cada caso para ver cómo puede ejecutarse ese derecho a la información de la manera más efectiva y más respetuosa con el otro bien jurídico que puede quedar afectado. Sobre todo habrá que estar a las características que presenta el receptor de la información y las circunstancias en las que se da esta información[1438]. Atendiendo a estas contingencias la información se podrá dar de una manera o de otra[1439].

II.3.2.B. La necesidad de flexibilizar en el ámbito sanitario la exigencia de que la información sea expresa, precisa e inequívoca.

Al hilo de lo que se acaba de señalar, la exigencia de rigurosidad en la forma de recabar la información, plantea en el ámbito sanitario una discusión de especial trascendencia. Más arriba se ha subrayado que las obligaciones impuestas por la LOPD para la protección de la persona en lo que a sus datos se refiere, tienen que compatibilizarse en el ámbito sanitario con el derecho del paciente a tener una asistencia médica efectiva y de calidad, y, sobre todo, con las necesidades de los profesionales sanitarios de manipular información para poder llevar a cabo su trabajo con la mayor eficacia posible[1440]. La necesidad de resolver la colisión entre la obligación de informar al titular sobre las características que van a rodear al tratamiento de sus datos y la exigencia de manipularlos de manera rápida y eficiente debería tener respuesta en una

[1438] APDCM, *Guía de Protección...*, cit., 2004, p. 117.

[1439] FERNÁNDEZ-SAMANIEGO y BERENGUER O´SHEA, "Recogida de datos…", cit., 2007, pp. 253-258, apunta, por ejemplo, los problemas que plantea el tener que cumplir con el deber de informar en el ámbito radiofónico, cuando se quieren recabar datos de oyentes que pretender participar en un concurso. Estos problemas prácticos llevan a que la información haya de darse de manera escalonada.

[1440] TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 93, reconoce la necesidad de adaptar el principio de información recogido en la LOPD a la realidad sanitaria para evitar una excesiva burocratización de la actividad asistencial.

norma concreta, dirigida a regular la protección de datos sanitarios[1441]. A falta de dicha norma, la solución tiene que venir de la ponderación en cada caso de los bienes jurídicos en juego.

La búsqueda de un equilibrio justo entre el derecho a la protección de la salud de manera eficiente y el derecho a la autodeterminación informativa tiene que llevar a realizar una interpretación del artículo 5 de la LOPD acorde a las circunstancias que rodean esta concreta situación. Las exigencias que la Ley establece para la defensa del derecho a la autodeterminación informativa no pueden obstaculizar la labor de los profesionales sanitarios, de tal manera que puedan llegar a poner en riesgo la salud y la integridad física y mental de los pacientes. En este sentido, no toda recogida de datos requiere de los mismos requisitos. Dentro del mismo ámbito sanitario, las diferentes circunstancias que pueden rodear a cada caso llevan a que haya que buscar fórmulas distintas para satisfacer el derecho a recibir la información oportuna. No es lo mismo la asistencia en un caso de urgencia, donde la rapidez juega un papel fundamental, y una consulta con el médico de cabecera, en la que puede haber más margen de tiempo para informar al usuario sobre los diferentes aspectos que pueden rodear al tratamiento de los datos que se van a manipular[1442].

Como punto de partida, atendiendo a la letra de la LOPD, en el ámbito sanitario hay que respetar el derecho de todo titular de datos a ser informado sobre los diferentes aspectos que van a rodear el tratamiento de los mismos de la forma que requiere la norma, cosa que en la práctica no siempre se hace, tal como ha señalado algún informe de la AEPD[1443]. Esta afirmación hay que entenderla, no obstante, dentro de la realidad de la Administración sanitaria y de las dificultades prácticas que a veces pueden surgir para poder llevar a cabo el derecho a la información.

Hay que plantear el deber de informar a los pacientes desde una perspectiva práctica[1444]. La información ha de ser expresa, precisa, inequívoca y completa, pero solamente todo lo expresa, precisa, inequívoca y completa que puede ser en un ámbito como el sanitario en el que la agilidad es fundamental. Hay que buscar, por lo tanto, una forma ágil de llevar a cabo la obligación de informar, pero que cumpla con los requerimientos de la Ley. Así pues, dentro del margen de actuación que concede el artículo 5 de dicha norma[1445], el cumplimiento de esta obligación se llevará a cabo de la manera más laxa posible, de tal forma que la práctica sanitaria pueda llevarse a cabo de la forma más rápida y eficaz posible.

Partiendo de lo dicho en el apartado anterior, pueden extraerse una serie de conclusiones. Si los datos de carácter sanitario se recaban a través de cuestionarios o formularios de otro tipo, la información habrá de aparecer de forma escrita y claramente legible, además de expresa, precisa, inequívoca y completa. Este apartado no genera grandes problemas, pues cuando los

[1441] TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 30, subraya que el derecho a la información "es un buen ejemplo de la dificultad de adaptar las exigencias de la legislación de protección de datos personales a las peculiaridades propias de la realidad sanitaria".
[1442] APDCM, *Guía de Protección...,* cit., 2004, p. 117.
[1443] Informe jurídico de la AEPD, "Informe de cumplimiento de la LOPD en Hospitales", octubre de 2010.
[1444] TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, pp. 1.154-1.155.
[1445] Respetando las exigencias de que la información se dé de forma expresa, precisa e inequívoca, que reclama el artículo 5.1 de la LOPD.

datos son recabados a través de esta fórmula en principio el propio medio favorece que la información pueda cumplir con las características comentadas. Esta información en los cuestionarios o demás formularios no puede sustituirse por información colocada en carteles o pósters en los centros sanitarios[1446].

Otra cosa ocurre cuando, como en la mayoría de los casos, los datos son recogidos por vías distintas a la citada. Como se ha dicho, en el ámbito sanitario la información no puede llevarse a cabo en cada acto asistencial, pues ello conllevaría un bloqueo del sistema. Atendiendo a esta circunstancia se ha propuesto antes que la información se dé de una forma más laxa que la que se podría exigir, en principio, atendiendo a los requisitos que dispone la normativa. De partida, la obligación de informar al titular de los datos sanitarios sobre las características que rodearán al tratamiento de los mismos puede verse satisfecha mediante una información genérica concerniente a esa manipulación de datos: las principales finalidades a las que se destinarán los tratamientos, facultades que integran el derecho a la autodeterminación informativa, responsables de los principales ficheros, obligación de los profesionales sanitarios de cumplir con el secreto… Esta información genérica puede darse en el comienzo de la relación entre el usuario y la Administración sanitaria. Podría llevarse a cabo mediante la entrega de un folleto formalizado, o vía oral mediante los propios profesionales sanitarios o a través de la información en el momento en que se hace entrega de la tarjeta sanitaria[1447]. Si bien ninguna de estas medidas excluye la posibilidad de aplicar las demás, la entrega de la tarjeta sanitaria podría constituir el momento más oportuno para llevar a cabo la información. Como se apuntaba más arriba, este instrumento integra datos de carácter personal, y en todo caso habrá de informarse al titular de los mismos, que será el usuario de la tarjeta, sobre el uso que se va a otorgar a esos datos[1448]. La información genérica a la que ahora se hace referencia se trataría de una información más o menos orientativa sobre las características generales que van a rodear al tratamiento de los datos del usuario.

Esta misma información, se podría decir genérica para todos los usuarios del sistema sanitario, habrá de mantenerse o repetirse cada cierto tiempo. Hay que tener en cuenta que la relación que vincula al usuario con la Administración sanitaria se alarga en el tiempo más allá incluso de la muerte del afectado. Así, hay que articular los medios oportunos para que dicha información genérica sea conocida de manera continua o repetida. Esto podría llevarse a cabo mediante el empleo de anuncios en los tablones, folletos informativos, información directa vía oral por los propios profesionales, que, como se ha apuntado, puede ser el personal auxiliar, pósters, etc[1449].

[1446] Resolución de la AEPD, R/00017/2008, 15 enero 2008, procedimiento PS/00231/2007.
[1447] SÁNCHEZ CARO y ABELLÁN, *Datos de Salud...,* cit., 2004, pp. 58-59.
[1448] Memoria AEPD, 1994: Consulta realizada por organismo público: "La Tarjeta Sanitaria como elemento identificativo con la posibilidad de incorporar el historial clínico.
La posibilidad de cifrar los datos que van incluidos en la tarjeta, sin el conocimiento del usuario atentaría gravemente contra el derecho a la información en la recogida de los datos, (...) dado que en este caso se estaría ocultando las consecuencias de la obtención de los datos, y además podrían acabar utilizándose los datos relativos a la salud en contra del propio afectado."
[1449] El Código Tipo de la Unió Catalana d´Hospitals, inscrito el 12 de julio de 2002, y modificado en julio de 2004, en su artículo 6.4 dispone que la obligación de informar se llevará a cabo a través de los siguientes medios: *"a. Entrega a*

Puede cuestionarse si esta información, más o menos genérica, cumple con los requisitos que exige la Ley[1450]. Los métodos que se acaban de citar han sido criticados por algún autor que ha tomado como argumento el hecho de que no cumplen los requisitos exigidos por la Ley[1451]. Si bien es cierto que se trata de una información genérica, dirigida a todos los usuarios, se entiende aquí que no atenta contra la letra de la LOPD. Se trata de una información concerniente a un tipo de tratamiento de datos, el tratamiento que exigen las operaciones sanitarias comunes a las que todo usuario está sujeto. Se informa de manera precisa, expresa, inequívoca y completa sobre los parámetros que rodean a este tipo de manipulación común. El empleo de esta fórmula encuentra apoyo en protocolos de actuación sanitaria que reconocen esta posibilidad como sistema de información[1452]. La Recomendación del Consejo de Europa[1453], a pesar de que en algún momento exige que la información sea individualizada[1454], dispone las vías de información comentadas como métodos válidos de cumplir con la obligación impuesta por la norma. Alguno de los informes jurídicos de la AEPD ha admitido también su validez[1455].

A esta información, se podría decir, genérica o común a todos, le ha de acompañar, como también se ha apuntado en el apartado anterior, una información más individualizada y concreta dirigida a cada usuario o paciente. Ésta se dará siempre y cuando los datos sanitarios del paciente vayan a ser objeto de una manipulación concreta que exija una nueva información que en la citada genérica no se ha podido dar. Principalmente se transmitirá cuando se produzca una cesión o la información se incluya en un nuevo fichero específico, distinto a los ficheros generales, como puede ser el caso de un fichero que contiene la información referida a los afectados por VIH. Evidentemente, en estos supuestos también se plantean los problemas que se han señalado anteriormente, especialmente la necesidad de tratar la información con rapidez y agilidad. No obstante, y siempre que no sea aplicable una excepción, se deberá encontrar la forma de llevar a cabo esta información individualizada de la mejor manera posible: mediante la

---

los usuarios de una hoja informativa con el contenido establecido en el anexo 2 de este código; b. Inserción en los folletos de información general del centro, en caso de haberlos, de una leyenda relativa a los extremos esenciales del documento contenido en el anexo 2 antes citado; c. Ubicación de paneles informativos en las áreas de admisiones y salas de espera de los centros con la leyenda que se establece en el anexo 3 de este código tipo"; APDCM, *Guía de...,* cit., 2004, p. 117. Informe jurídico AEPD, 0304/2005. CANALES GIL, "Derecho de información…", cit., 2010, p. 413, reconoce la posibilidad de emplear carteles como método de cumplir el deber de informar en el ámbito sanitario.

[1450] LÓPEZ, MOYA, MARIMÓN, y PLANAS, *Protección de Datos...,* cit., 2001, p. 12.

[1451] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 38.

[1452] Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España, inscrito el 12 de julio 2004, y modificado el 2006; artículo 10: "Se informará al paciente o usuario de los servicios de salud bucodental de la recogida de sus datos. Dicha información deberá de realizarse por alguno de los medios siguientes, en la anámnesis entregada al inicio de la relación con el paciente o usuario de los servicios de salud bucodental y/o, en un cartel a la vista del público en la recepción de pacientes, o en los vestíbulos y/o salas de espera de las clínicas y/o consultorios dentales individuales o colectivos de los Adheridos al Código."

[1453] Punto 111 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa.

[1454] Artículo 5.3 R (97) 5.

[1455] Informe jurídico 0304/2005, AEPD, sobre diferentes cuestiones relativas a la Historia Clínica: "esta Agencia ha venido considerando suficiente el cumplimiento del deber de información mediante la existencia de un cartel anunciador siempre que el mismo resulte claramente visible por parte del afectado, quedando así garantizado que el mismo ha podido tener perfecto conocimiento de la información exigible.

Igualmente, podría optarse por la inclusión de la cláusula informativa en un impreso, que fuera entregado al afectado, siempre que se acreditase que el mismo ha sido debidamente informado sobre el tratamiento y cesión de sus datos, por ejemplo, mediante su firma.

De este modo la solución planteada en la consulta resultaría admisible, siempre que el cartel reúna los requisitos de ubicación y formato que garanticen su conocimiento por parte de los interesados".

remisión de información a los hogares de los usuarios, acoplando o adicionando la información que pide la LOPD al requerimiento de consentimiento informado para el tratamiento sanitario[1456], etc.

Esta información individualizada cumple con mayor vigor los requisitos que exige la Ley y es el complemento ideal a la comentada información genérica. Se dirige a aclarar aspectos concretos sobre una manipulación o uso determinado de algunos datos del usuario o paciente. No obstante, hay que subrayar de nuevo, este tipo de información se llevará a cabo en casos o circunstancias en que se estime necesario, pues en muchos supuestos la necesidad u obligación de informar quedará cubierta por la primera información genérica. Además habrá de tenerse presente, que dependiendo de la forma en que se han recabado los datos, si la fuente es el propio usuario o no, la información deberá darse en el momento de la recogida o, dentro de un plazo máximo de tres meses, lo antes posible, respectivamente.

II.3.3. Los elementos sobre los que hay que informar.

En el apartado anterior se ha indicado que la información que el responsable ha de transmitir al titular de los datos ha de ser completa. Este calificativo se refiere al contenido de la información que se tiene que dar.

II.3.3.A. Sobre la necesidad de que la información sea lo más completa y concreta posible.

Se deberá informar al titular de los datos de prácticamente todos los parámetros que rodearán al tratamiento de los mismos. Las normas están, en líneas generales, de acuerdo al señalar que el contenido deberá referirse cuando menos a los siguientes aspectos: a)la existencia del fichero o tratamiento, la finalidad de la recogida y de los destinatarios de la información; b) del carácter obligatorio o facultativo de su respuesta a las preguntas que se plantean; c) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; d) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y e) de la identidad y dirección del responsable del tratamiento o de su representante. Como se puede apreciar, el legislador pretende que el titular de los datos pueda tener una perspectiva completa a la hora de dar su consentimiento para que sus datos sean manipulados, o simplemente para que tenga conocimiento de cómo va a desarrollarse dicha manipulación.

Los elementos sobre los que hay que informar son diversos. Sin embargo, la importancia de informar sobre unos u otros no es la misma. Hay puntos cuyo conocimiento es más relevante que otros.

Sin duda, como medio de control sobre los datos de cada uno, el conocer las finalidades y los destinatarios a los que van a ser dirigidos los datos constituye un elemento fundamental. Así lo han entendido también la jurisprudencia[1457], la doctrina[1458] y la AEPD en sus resoluciones[1459]. Lo

[1456] MARTÍNEZ-CAMPELLO, "La Ley 41/2002...", cit., 2004, pp. 180-181.
[1457] STC 30 de noviembre del 2000: "ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quien dispone de esos datos personales y a qué usos los está sometiendo (...)".
[1458] GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 251: p. 252.

mismo ocurre con la información sobre la posibilidad de ejercer los derechos de acceso, cancelación, rectificación y oposición respectivamente: la posibilidad de ejercer estas facultades pasa, en primer lugar, porque se informe al titular de los datos sobre cómo llevarlas a cabo. El conocimiento de esta información, frente al conocimiento de otros puntos como puede ser el hecho de que la respuesta a unas preguntas sea facultativa o no, se antoja de especial importancia. Realmente, puede afirmarse que el derecho a la información quedaría vacío de contenido si se excluyeran de esa información los puntos sobre la finalidad, los posibles destinatarios de los datos y la posibilidad de ejercer los derechos de acceso, cancelación y rectificación[1460]. Este apunte tiene su relevancia por cuanto en algunos casos, cuando la información se va a llevar a cabo en ámbitos tan complejos como el de la sanidad, que requiere de cierta flexibilidad, se podrá prescindir de alguna información, pero no de los puntos más relevantes.

Especial mención hay que hacer de la información sobre la finalidad. Ya se ha dicho, en el capítulo referente a los principios que determinan la calidad de los datos, que el principio de finalidad constituye uno de los elementos vertebradores del régimen protector del derecho a la autodeterminación informativa. Tanto cuando en la manipulación de los datos se requiere el consentimiento del afectado como cuando éste resulta excluido, la finalidad se erige en el parámetro determinante a la hora de delimitar el marco dentro del que el tratamiento se puede realizar. La manipulación de datos no puede ir más allá de la finalidad marcada. En este sentido, a la hora de informar sobre la finalidad, en numerosas ocasiones la AEPD ha hecho hincapié en la necesidad de que esta información sea lo más concreta posible, sin que quepan informaciones genéricas sobre la misma[1461].

En relación a la necesidad de que la finalidad sea concreta y precisa, la doctrina no parece haberse puesto de acuerdo. Hay quien entiende que basta con informar sobre la finalidad de manera más o menos genérica para comprender que la obligación de informar está cumplida[1462]. Otra parte de la doctrina ha subrayado, se cree aquí que acertadamente, la necesidad de que la finalidad sea lo más precisa y concreta posible[1463]. Esta interpretación está plenamente justificada. Si el derecho a la autodeterminación informativa consiste en el pleno control de la persona sobre los datos que le conciernen, es razonable pensar que para que dicho control sea

[1459] Resolución AEPD, 00647/2005, 5 septiembre de 2005, procedimiento PS 00053/2005: "De su literalidad no se aprecia que exista información sobre finalidades determinadas y explícitas a las que se vinculará el tratamiento de los datos pues se limita a el término finalidad "*comercial"*, que, por su extraordinaria amplitud, según el Diccionario de la Lengua "*perteneciente al comercio y a los comerciantes",* no explicita con una determinación suficiente la información que previamente debe ser conocida por lo clientes". "Por otra parte, la referencia a "*cesión de datos a las distintas empresas del Grupo Pelayo",* es, asimismo indeterminada pues no concreta quienes van a ser los destinatarios de la información"; STC 292/2000, 30 noviembre, "el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de estos, pues sólo así será eficaz su derecho a consentir".

[1460] Resolución AEPD 00451/2005, 20 junio de 2005, procedimiento AAPP/00029/2004.

[1461] Resolución AEPD 00288/2006, 9 de mayo de 2006, procedimiento AAPP/00050/2005.

[1462] GUICHOT, *Datos Personales...*, cit., 2005, p. 386, pie de página 642: "APARICIO SALOM considera que la finalidad de la que debe ser informado es la abstracta, o genérica (...) y no la específica. Ahora bien, creemos que la expresión de una finalidad tal no satisface el requisito de finalidad expresa y determinada"; APARICIO SALOM, *Protección de Datos…,* cit., 2009, p. 173.

[1463] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 38; CANALES GIL, "Derecho de información…", cit., 2010, p. 408.

efectivo, el titular de los datos deberá conocer, tanto si tiene que consentir la manipulación o no, la finalidad específica que se persigue con dicho tratamiento. No basta con una finalidad genérica o indeterminada. Piénsese, por ejemplo, en el supuesto en que se va a llevar a cabo un contrato con una compañía telefónica o una entidad bancaria y se le informa al cliente que sus datos van a ser empleados con la finalidad de prestar un buen servicio. Parece claro que esa información no es suficiente. Habrá de concretarse a qué finalidades específicas se va a dirigir el tratamiento de los datos: publicidad, estudios estadísticos, prestación de un servicio determinado, etc.

El principal elemento de controversia respecto al contenido que ha de tener la información lo constituye otro punto: el saber si la información que hay que transmitir al titular de los datos ha de incluir también la relativa a las futuras cesiones que se vayan a realizar de los datos que se van a manipular. La LOPD no reconoce de manera expresa la obligación de informar sobre las cesiones de datos que el responsable del fichero pueda tener previstas. Sin embargo, dicha obligación puede deducirse, a pesar de que en algún caso no se haya hecho así[1464], de la lectura de otros preceptos de la norma[1465].

La misma disposición que regula el derecho que se analiza reconoce la necesidad de informar sobre los destinatarios de la información que se recaba[1466]. Indudablemente, si se ha de informar sobre los destinatarios se deberá de informar sobre las cesiones que se tienen previstas, pues éstas constituyen la trasmisión de los datos a nuevos destinatarios. Por otro lado, al regular la comunicación de los datos también se deja entrever la voluntad del legislador de que se informe sobre las cesiones que se van a llevar a cabo en el tratamiento de los datos. La Ley, en la regulación de la comunicación de datos de ficheros privados, exige que se informe al afectado, en el momento en que se realice la primera cesión, sobre la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario[1467].

De estos preceptos puede deducirse la voluntad del legislador de que, como norma general, se le informe al titular de los datos sobre las comunicaciones que se van a llevar a cabo en relación a los mismos. Si el sentido último del derecho a recibir la información es tener un fundamento o argumento necesario para poder autorizar o no el tratamiento de unos datos, o, en caso de que esta autorización o consentimiento no sea necesario, salvaguardar un espacio mínimo de control del afectado por el tratamiento, hay que entender que el titular debe conocer algo tan relevante como las cesiones que se tienen previstas sobre sus datos. En esta misma línea, la propia jurisprudencia reconoce sin ambages la necesidad de informar sobre las cesiones previstas para que la citada información sea completa[1468]. Así lo hace también la Recomendación del Consejo de Europa de protección de datos médicos[1469].

[1464] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, 175.
[1465] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 39.
[1466] Artículo 5.1.a) LOPD.
[1467] Artículo 27.1 LOPD.
[1468] STC de 30 de noviembre de 2000, FJ 13: "es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales".
[1469] Artículo 5.1.d) R (97) 5: "*Los afectados deberán ser informados de los siguientes aspectos: d) las personas u órganos a los que pueden ser comunicados y con qué fines".*

Respecto a la necesidad de informar sobre las futuras cesiones la Ley no fija el momento en que ha de llevarse a cabo dicha información. En este punto podría plantearse una contradicción entre diferentes preceptos de la LOPD. El artículo 5 de la Ley obliga a llevar a cabo la información en el momento de la recogida, cuando los datos son recabados del titular, o lo antes posible y a más tardar en el plazo de tres meses, cuando los datos son recabados de fuente distinta al titular de los datos. Por su parte, las disposiciones dirigidas a la regulación de la comunicación de los datos contenidos en ficheros privados obligan a informar sobre las características de la cesión, pero en el momento de llevar a cabo la citada comunicación. Según esta última previsión la información no será necesaria hasta que se produzca la comunicación. Por lo tanto, se plantea la cuestión de si la información sobre la cesión ha de llevarse a cabo tal y como lo exige el artículo 5 o como lo recogen las disposiciones relativas a la comunicación de datos. La solución puede venir de un planteamiento que aúne ambas disposiciones.

El hecho de que se tenga que informar de la cesión en el momento en que ésta se produzca no significa que antes, en la recogida, no haya tenido que informársele sobre la posibilidad de llevar a cabo dicha operación en un futuro. Siguiendo a parte de la doctrina[1470] se puede entender que el derecho a dar un consentimiento informado exige que se informe al afectado en el momento mismo de la recogida de los datos sobre las posibles cesiones que se vayan a dar. La autorización del titular deberá basarse en la información más completa posible. La misma conclusión se desprende también, como se ha dicho, de la Ley, cuando se exige que se informe al afectado sobre la finalidad y los posibles destinatarios de los datos. Si en el momento de la recogida de los datos el responsable del fichero tiene que informar al titular sobre todos los destinatarios de la información, necesariamente tendrá que darle a conocer las posibles cesiones que se pretenden llevar a cabo. Las cesiones que están previstas por el responsable del fichero en el momento de recoger los datos de carácter personal tienen que ser comunicadas al titular de los datos junto al resto de elementos sobre los que se ha de informar. Esta misma idea se deduce del hecho de que cuando la Ley regula la creación de los ficheros tanto públicos como privados, se obliga a los responsables a incluir las cesiones previstas dentro de la información que se ha de transmitir a la agencia correspondiente[1471]. Evidentemente, si ya en el momento de la creación de los ficheros se exige al responsable la inclusión de la información sobre las cesiones previstas, parece lógico pensar que esa misma información deberá darse al titular de los datos lo antes posible. No obstante, lo dicho no quita para que cuando la cesión efectivamente se lleve a cabo, o se pretendan cesiones que no estaban previstas cuando los datos se recabaron, se le informe también al afectado. Y es que, la cesión constituye un nuevo

[1470] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, pp. 236-241.

[1471] Artículo 26 LOPD: "*1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.*
2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros"; Artículo 20.2, LOPD: "*Las disposiciones de creación o de modificación de ficheros deberán indicar: (...) e) las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros*".

tratamiento de los datos que ha de ser aprobada por el titular de los mismos, aprobación que, como ya se dijera, requiere de la previa información.

II.3.3.B. Una propuesta sobre la forma de llevar a cabo una información completa y concreta en el ámbito sanitario.

La obligación de informar de una forma completa es aplicable también al sector sanitario. En algún caso la AEPD ha sancionado un tratamiento de datos en este ámbito por el incumplimiento de este deber de informar al emplear en la información cláusulas genéricas[1472]. ¿Qué información ha de otorgarse al usuario del sistema sanitario en relación al tratamiento que van a sufrir sus datos?

En principio, como en todos los ámbitos en que se manipulan datos de carácter personal, es necesario que al usuario del sistema sanitario se le informe de los aspectos que recoge la Ley. Sin embargo, si se atiende a la normativa interna de la Administración sanitaria y a los protocolos de actuación de determinados centros, se puede observar que el contenido de la información que reconoce la LOPD se completa con otra información que no recoge esta Ley. Ciertamente, si se tienen en cuenta las particularidades que presenta la práctica sanitaria, parece recomendable informar sobre más aspectos que los que la norma establece.

La conocida Circular del INSALUD de protección de datos añade a la comentada la información sobre el derecho del paciente a no confesar o declarar su religión, creencias o ideología[1473]. Se trata de un derecho reconocido en la propia CE[1474] y sobre el que tiene pleno sentido informar teniendo en cuenta las circunstancias que se pueden dar en la práctica sanitaria. Piénsese en casos en que la religión de una persona le impide recibir un tratamiento determinado. Cierto es que el valor jurídico de la circular es limitado de cara al ámbito externo de la Administración en la que se dicta[1475], sin embargo, en el ámbito interno marca una línea de interpretación de la LOPD que los profesionales sanitarios tienen que seguir.

Por otro lado, en algún código tipo se ha recogido la obligación de informar sobre la vinculación de los profesionales sanitarios a dicho protocolo y la posibilidad de todo usuario de obtener una copia del mismo[1476]. Esta información tiene también su utilidad en la medida en que ofrece cierta seguridad al ciudadano de que el profesional está sujeto a las normas de protección de datos.

[1472] Resolución AEPD, R/00711/2005, 3 de octubre de 2005, procedimiento PS/00018/2005, determinaba que la información no era acorde a Derecho debido a que apuntaba la posibilidad de realizar cesiones en el ámbito sanitario, sin concretar los destinatarios.
[1473] Artículo 9.1.g) Circular 9/97, 9 de julio 1997.
[1474] Artículo 16.2 CE.
[1475] LASAGABASTER HERRARTE, *Fuentes del Derecho...,* cit., 2007, p. 193: "la circular no es una norma reglamentaria, no vincula a tribunales y particulares, aunque sí a la propia Administración".
[1476] Artículo 13.h) Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España, inscrito el 12 de julio 2004, y modificado el 2006: dispone la obligación de informar "Que el Odontólogo o Estomatólogo está adherido al Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España y que dispone de una copia del Código Tipo para su consulta".

Por último, en sectores específicos de la sanidad como es el de la investigación la regulación exige también una información complementaria a la requerida por la Ley: advertencias sobre la posibilidad de que mediante la manipulación de la información se lleguen a conocer aspectos desconocidos del paciente, información sobre la obligación de secreto del profesional, etc.[1477].

El contenido sobre el que hay que informar en el ámbito sanitario es, por lo tanto, extenso. La excesiva extensión de la información ha planteado dudas en este ámbito cuando se trata de la información referida, no a los parámetros que ha de guardar la manipulación de datos, sino a las características del tratamiento médico que se vaya a dar al paciente. Refiriéndose a esta información sobre el estado de salud del usuario y sobre el cuidado médico a seguir, la jurisprudencia ha señalado en más de una ocasión que una excesiva información puede llegar a complicar la relación entre el profesional sanitario y el paciente, y que puede ser a veces perjudicial para este último[1478]. En este sentido señalan la jurisprudencia[1479] y la doctrina[1480] que basta, en principio, con una información suficiente.

En el ámbito de la protección de datos no se está hablando sobre informar al paciente de su estado de salud ni de las características del tratamiento médico que se le puede impartir, sino sobre las características del tratamiento que se va hacer de los datos sanitarios. Parece claro que una información detallada sobre las circunstancias que van a rodear la manipulación de los datos del paciente no puede afectar a este último de manera negativa en su relación con el profesional sanitario. Es más, se entiende que una buena información en este ámbito salvaguarda de una manera más eficiente el derecho a la autodeterminación informativa, lo que puede redundar en una mejor relación entre profesional sanitario y paciente.

La información ha de ser lo más completa y detallada posible. Esta exigencia plantea, sin embargo, la dificultad de llevarla a cabo. Antes se ha hablado de la posibilidad de otorgar a los usuarios del sistema sanitario una información primero genérica y luego individualizada sobre cómo va a desarrollarse el tratamiento de sus datos en este ámbito.

La información genérica podía llevarse a cabo a través de carteles, folletos, etc., y a ella podrían acceder, de una u otra forma, todos los usuarios del sistema sanitario. Desde el punto de vista del contenido esta información genérica puede comprender elementos de gran interés. Sin duda, se puede llevar a cabo en esta información un acercamiento a las posibles finalidades y los posibles destinatarios que puede tener la manipulación de datos: la investigación, la docencia, el uso de los datos con fines judiciales, la estadística, etc. Se puede informar también en esta información genérica, sobre la cualidad de obligatoria o facultativa de la información que puede transmitir el usuario: salvo contadas ocasiones, la recogida de información es voluntaria. De la misma forma, es completamente plausible a través de estos medios la información sobre las

[1477] Artículos 15, 47 y 59 Ley 14/2007, 3 de julio, Investigación Biomédica.
[1478] STS 9 noviembre 2005, FJ 5.
[1479] STS 26 de junio 2006, FJ 5.
[1480] CANTERO MARTÍNEZ, *La Autonomía...*, cit., 2005, p. 22: "si la falta de información puede viciar la válida prestación del consentimiento, la información excesiva puede convertir la atención clínica en desmesurada y en un padecimiento innecesario para el enfermo y, en todo caso, no se trata de que el paciente reciba un curso de medicina acelerada".

consecuencias que puede acarrear la no obtención por los profesionales sanitarios de una información adecuada y suficiente en el desarrollo de la actividad sanitaria. Este punto tiene especial importancia en el ámbito sanitario, pues ya se ha repetido en diferentes ocasiones la gran relevancia que tiene una información de calidad para el tratamiento sanitario. Precisamente, el anteriormente citado protocolo de actuación hace hincapié en la necesidad de informar a los usuarios sobre la importancia de que transmitan los datos a los profesionales que les van a atender de forma veraz y completa[1481]. Pues bien, esta advertencia puede llevarse a cabo también a través de la citada información genérica. La información sobre las posibilidades de ejercer los derechos de acceso, cancelación y rectificación también puede llevarse a cabo mediante este tipo de información. Cierto es que, como se verá, el ejercicio de estos derechos plantea en el ámbito sanitario muchas interrogantes y que la información sobre la existencia de los mismos no podrá ser especialmente precisa y detallada, explicando cómo pueden ejercerse estos derechos en cada caso o circunstancia. No obstante, puede comunicarse a los usuarios la posibilidad general de ejercer estos derechos y la forma de llevar a cabo los mismos. En relación a la información sobre estas facultades de acceso, cancelación o rectificación, conviene también informar al titular de los datos sobre la importancia de su ejercicio para mantener la calidad de los mismos, lo que redundará en última instancia en beneficio de una buena asistencia sanitaria.

La referida información dará una perspectiva general de cómo va a desarrollarse el tratamiento de los datos de los usuarios en el sistema sanitario. Se entiende que esta información ha de ser todo lo detallada y precisa que pueda ser. No se puede exigir que se refiera a todas las situaciones que pueden generarse en la práctica sanitaria, puesto que cada caso individual irá planteando nuevas situaciones sobre las que habrá que informar, y que la información genérica a la que ahora se hace referencia no puede prever todas estas circunstancias. Es por ello que a la información genérica habrá de acompañarle la información individualizada que recoja los datos sobre las circunstancias particulares del tratamiento de cada usuario.

La información individualizada no exige, sin embargo, que se informe de manera detallada en cada acto sanitario sobre todas las características que exige la Ley. Esto no tendría sentido en la práctica, pues la mayor parte de los actos, en la medida en que no conllevan nuevos tratamientos de datos, requieren de la misma información. Piénsese que la mayoría de las veces, cuando se acude al médico de cabecera, la información que se otorga en cada acto no plantea circunstancias nuevas sobre las que haya que informar. Esa información la cubre, salvo circunstancias especiales, la información genérica que se ha citado. No obstante, puede ocurrir que a esos actos acompañen actos específicos que planteen nuevos elementos sobre los que haya que informar: cesiones a otras entidades sobre las que habrá que informar al titular de los datos, creación de ficheros específicos con fines concretos como es el caso del citado SINIVIH o

[1481] Artículo 13.g) Código Tipo de Tratamiento de Datos de Carácter Personal para Odontólogos y Estomatólogos de España, inscrito el 12 de julio 2004, y modificado el 2006: a los elementos que reconoce la LOPD sobre los que hay que informar se les añade o suma: "Que los pacientes o usuarios de los servicios de salud bucodental tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razón de interés público o con motivo de la prestación del servicio de odontología o estomatología".

fichero relativo al Sistema de Información de Nuevas Infecciones, etc[1482]. Para estos casos que podrían calificarse como nuevos tratamientos de datos, los requisitos de que la información sea expresa, precisa, inequívoca y completa entran con todo el vigor que requiere la Ley.

II.4. Las excepciones al derecho a ser informado.

II.4.1. Aspectos generales de las excepciones al derecho a la autodeterminación informativa.

Como se ha visto, el respeto al derecho a la autodeterminación informativa integra como parte fundamental de su contenido la exigencia de que el responsable del fichero remita al titular de los datos la información pertinente sobre las características del tratamiento de datos que pretende. No obstante, a esta primera regulación acompañan situaciones previstas por la Ley para las que el derecho a la información queda exceptuado[1483]. Se analizarán ahora dichas excepciones. Se trata del aspecto más problemático de la regulación del derecho a la información, pues en la norma se prevén excepciones que debido sobre todo a su ambigüedad pueden llegar a vaciar de contenido el derecho que previamente se ha reconocido.

A la hora de analizar estas excepciones, hay que tener en cuenta que los límites al derecho a ser informado que prevé la LOPD son aplicables a todo tipo de tratamiento, a toda esfera de la realidad donde los datos puedan ser tratados. La Ley no entra a analizar las características de cada ámbito de la realidad, como el sanitario, para que la aplicación de dichos límites se adecue de manera correcta a sus características propias. El problema es que en el ordenamiento jurídico no hay norma alguna que lleve a cabo ese ejercicio de acomodación de la Ley a la realidad sanitaria. Esto hace que la LOPD presente un sistema de excepciones al derecho a ser informado especialmente ambiguo que genera problemas a la hora de ser aplicado por los profesionales sanitarios. Las dificultades de adaptación de la letra de la Ley a la práctica sanitaria son, como se verá, evidentes. Precisamente debido a esta circunstancia, la doctrina ha llegado a realizar interpretaciones muy variadas de dichas excepciones. Hay quien incluso ha llevado a cabo una interpretación propia sobre la aplicación de las excepciones al derecho a la información en el ámbito sanitario, olvidándose prácticamente de lo que dicta la Ley[1484]. Se tratará en este momento de arrojar un poco de luz sobre esta cuestión. Para ello habrá que tener en cuenta que la perspectiva con la que hay que interpretar estas excepciones, cuando se trata de analizar la manipulación de los datos en un sector tan complejo como el sanitario, ha de ser necesariamente

[1482] Orden 18 de diciembre de 2000 por la que se crea un fichero con datos de carácter personal, gestionado por el Ministerio de Sanidad y Consumo, relativo al Sistema de Información sobre Nuevas Infecciones, BOE nº 11, 12 de enero 2001.

[1483] SÁNCHEZ CARAZO, *La Intimidad...*, cit., 2000, pp. 135-138, realiza un interesante análisis sobre las excepciones que las diferentes normas disponen al derecho a la información.

[1484] SÁNCHEZ CARAZO, *La intimidad...*, cit., 2000, p. 134: en relación a las excepciones que fija la Ley al derecho a la información: "Creemos que tanto lo que dice la Ley Orgánica 15/1999, como lo expuesto por el autor anterior introduce algunas excepciones que son válidas para el derecho-deber del consentimiento pero no en lo referente a la información. Pensamos que la obligación de informar sobre cualquier tratamiento de datos es tan absoluta que sólo podría decaer en tres casos: 1. Cuando el enfermo no quiera ser informado, utilizando su derecho a no saber, situación también prevista en el Convenio relativo a los Derechos Humanos y la Biomedicina. 2. Cuando la urgencia terapéutica, siguiendo el principio de beneficencia a favor del enfermo, asó lo requiera, y sólo mientras dure esa urgencia. 3. Cuando la información sobre el interesado se encuentra *inseparablemente* unida a la información sobre otra u otras personas".

distinta a la que se emplea para analizar el tratamiento de los datos en la mayoría de los demás sectores de la vida.

En el ámbito que se estudia, la relación que se da entre el titular de los datos y el responsable del fichero es realmente compleja: se trata de una relación que se alarga en el tiempo; los bienes jurídicos que entran en conflicto son numerosos; la necesidad de tratar los datos con agilidad y rapidez es notable, etc. Como se ha dicho al estudiar el contenido de dicho derecho, la agilidad que la práctica sanitaria requiere en el tratamiento de los datos hace que los requisitos que exige la realización efectiva del derecho a ser informado tengan que ser analizados de forma flexible. Lo mismo ocurre con las excepciones. La necesidad de una ágil manipulación de la información sanitaria y, en algunos casos, la imposibilidad física de poder llevar a cabo la información en el momento de la recogida de los datos, hace que sea posible la aplicación de estas excepciones[1485]. El estricto cumplimiento de la obligación de informar puede llevar a una atrofia del sistema sanitario[1486]. Sin embargo, este hecho tampoco puede justificar una interpretación amplia de los límites. Hay que tratar de buscar un equilibrio entre el cumplimiento efectivo del derecho a la información y la posibilidad de ejercer la práctica sanitaria de forma ágil y efectiva. Las excepciones que ahora se van a analizar deben comprenderse e interpretarse dentro de este marco.

Antes de pasar a estudiar las excepciones que la Ley prevé para el derecho a ser informado merece la pena exponer, aunque sea brevemente, algunos argumentos que ayudarán a comprender mejor los límites no sólo a este derecho, sino también a cualquier otra de las facultades que compone el derecho a la autodeterminación informativa. Es decir, se tratará de fijar unos criterios que todo límite al citado derecho ha de cumplir para que se entienda como válido. Estos requisitos vienen fijados, sobre todo, por la jurisprudencia del TC y del TEDH, si bien desde diferentes instancias se han llevado a cabo aportaciones de interés.

Como punto de partida se puede atender a la consideración que lleva a cabo el TC, hoy plenamente asumida, de que todo límite a los derechos fundamentales tiene que basarse de manera directa o indirecta en los superiores valores que la Constitución reconoce en su articulado[1487]. Por lo tanto, el límite a un derecho fundamental sólo podrá sustentarse en un bien jurídico de especial relevancia. Asumiendo la jurisprudencia que se acaba de citar, expuesta por el Tribunal con mucha prontitud[1488], lo esencial en este momento es determinar hasta dónde pueden llegar esos límites en un caso tan complejo como el del derecho fundamental que aquí se analiza.

Los límites al derecho fundamental tienen que cumplir con requisitos que aseguren la seguridad jurídica y garanticen, en base al principio de justicia, el equilibrio entre las libertades y

[1485] SÁNCHEZ CARO y ABELLÁN, *Datos de Salud...,* cit., 2004, p. 60.
[1486] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 187.
[1487] STC de 26 de noviembre de 1984, en la que se analiza el alcance de la facultad de la Administración Tributaria para investigar los datos relativos a la situación económica de los ciudadanos: "todo derecho tiene sus límites que en relación a los Derechos Fundamentales establece la Constitución por sí misma en algunas ocasiones, mientras en otras el límite deriva de manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionales protegidos".
[1488] STC 8 abril de 1981.

los derechos fundamentales, y demás bienes jurídicos a proteger reconocidos en la norma suprema.

En primer lugar, señala la jurisprudencia que a la hora de interpretar los límites de los derechos fundamentales no puede llevarse a cabo una interpretación expansiva de los mismos. Es decir, las excepciones a los derechos fundamentales deberán interpretarse de manera estricta, sin que se pueda estirar la letra de la Ley para incorporar nuevos límites o ampliar el sentido de los que la norma recoge[1489]. La posibilidad de llevar a cabo interpretaciones amplias de los límites, señala el TC, conlleva un alto riesgo de abrir la puerta a actuaciones que pueden atentar contra el núcleo esencial de estos derechos.

En segundo lugar, y partiendo del marco general que se acaba de exponer, la jurisprudencia ha señalado otra serie de requisitos que todo límite al derecho a la autodeterminación informativa ha de cumplir. La jurisprudencia ha analizado el enfrentamiento entre el derecho a la autodeterminación informativa y la salvaguarda de la salud de los ciudadanos, y ha establecido los criterios que se han de seguir para la búsqueda del equilibrio entre estos dos intereses[1490]. La AN ha puesto en cuestión la validez de una orden que crea un fichero con datos de personas infectadas con el VIH[1491]. El objetivo fundamental de esa orden es el de prevenir, gestionar y prestar servicios sanitarios a enfermos con VIH y SIDA, y preservar y promocionar la salud de la población, así como controlar los procesos de transmisión y otros procesos agudos de interés sanitario, y con ese fin se crean ficheros con datos de carácter personal sanitarios. Es de entender que se trata de datos especialmente sensibles, pues su conocimiento por parte, por ejemplo, de empresas y aseguradoras, podría acarrear efectos realmente perversos. Partiendo de estos elementos la audiencia se pregunta si es posible que en determinadas situaciones se permita a los poderes públicos limitar derechos fundamentales de los ciudadanos en beneficio de la protección de la salud de la ciudadanía. Trata de ponderar los bienes jurídicos en juego para poder cumplir con la finalidad citada afectando lo menos posible al derecho fundamental a la autodeterminación informativa[1492]. Precisamente, para llevar a cabo este ejercicio de ponderación, la audiencia recurre a los parámetros marcados por el TEDH, que establece tres requisitos a los que toda injerencia a la vida privada debe quedar sujeta: tener una base legal (previsibilidad), perseguir un fin legítimo (fin justificado) y ser una medida necesaria en una sociedad democrática (proporcionalidad).

Lo expuesto lleva necesariamente a tener que acudir a las interpretaciones que el TEDH sobre todo[1493], pero también el TJUE, han realizado de los conceptos de previsibilidad, fin justificado y proporcionalidad.

[1489] SAN 26 de septiembre de 2002, FJ 3. "las excepciones (...) deben ser interpretadas de modo estricto sin que quepa admitir otros casos de dispensa del consentimiento distintos al que aparece expresamente contemplado en la norma"
[1490] STS 9 julio 2007, anula la SAN 24 de marzo de 2004, si bien esta anulación no afecta a la coherencia de los argumentos de la AN con respecto a las características que han de cumplir los límites de los derechos fundamentales.
[1491] Orden del Ministerio de Sanidad y Consumo de 18 de diciembre de 2000, por la que se crea un fichero con datos de carácter personal relativo al Sistema de Información sobre Nuevas Infecciones (SINIVIH).
[1492] SAN 24 de marzo de 2004, FJ 8.
[1493] ARZOZ SANTIESTEBAN, "Artículo 8...", cit., 2004, pp. 254-328.

El TJUE en más de una sentencia se ha dedicado a analizar la cuestión de la protección de datos. Normalmente, para aplicar la Directiva europea reguladora de esta materia, emplea los criterios de interpretación fijados por el TEDH con respecto del artículo 8 del CEDH[1494]. Según este Convenio la autoridad pública podrá llevar a cabo una injerencia en el ámbito de la vida privada de los individuos siempre que esté prevista por la Ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros[1495].

En cuanto a la previsibilidad por la ley, apunta el TEDH que esta expresión no supone simplemente una remisión a la Ley, sino que hace referencia también a la "calidad de la Ley". Se entiende que la norma que recoge la limitación del derecho fundamental ha de ser accesible para los ciudadanos a los que va dirigida[1496], es decir, lo suficientemente clara y precisa como para que los ciudadanos conozcan con detalle en qué términos se aplica dicha excepción: en qué circunstancias y mediante qué requisitos[1497]. Esta premisa exige que la Ley deje claro el alcance de la limitación y las modalidades de su aplicación[1498]. El grado de detalle al que el derecho interno tiene que llegar al fijar un límite es, según se desprende de la jurisprudencia del TEDH, bastante alto[1499]. En los mismos términos parece expresarse el TJUE cuando señala que este requisito hace referencia no al hecho de que la injerencia esté recogida en una norma, sino a la necesidad de que la norma esté redactada con la suficiente precisión como para que "los destinatarios de la Ley adapten su conducta"[1500]. En este sentido, la propia Directiva europea de protección de datos, refiriéndose al consentimiento, y más concretamente a la regulación de esta figura en el ámbito sanitario, subraya la necesidad de que las excepciones a éste se fijen de forma explícita[1501] de manera que no quepa duda alguna sobre la identidad y extensión de la excepción.

En cuanto al segundo requisito exigido por el Convenio para que una intromisión en la vida privada sea legítima, el TEDH lleva a cabo apreciaciones muy claras. Para que un límite a este derecho se considere "necesario en una sociedad democrática", el tribunal arriba citado requiere

[1494] STJUE de 20 de mayo de 2003, Rechnungsof y otros v. Österreichischer Rundfunk y otros, asuntos acumulados C-465/00, C-138/01 y C-139/91, FJ. 72.
[1495] Artículo 8 CEDH.
[1496] STEDH de 26 de marzo de 1987, Caso Leander. FFJJ 50 y 51.
[1497] STEDH de 2 de agosto de 1984, Caso Malone contra Reino Unido, FJ 67.
[1498] STEDH de 2 de agosto de 1984, Caso Malone contra Reino Unido, FJ 68. STEDH, de 30 de julio de 1998, Caso Valenzuela Contreras contra España, FJ 46.
[1499] STEDH de 30 de julio de 1998, Caso Valenzuela Contreras contra España, FJ 46. "Como garantías mínimas, necesarias para evitar los abusos, que deben figurar en la Ley, las Sentencias Kruslin y Huvig, mencionan: la definición de las categorías de personas susceptibles de ser sometidas a vigilancia telefónica judicial; la naturaleza de las infracciones a que puedan dar lugar; la fijación de un límite a la duración de la ejecución de la medida; las condiciones de establecimiento de los atestados que consignen las conversaciones interceptadas; las precauciones que se deben tomar para comunicar, intactas y completas, las grabaciones realizadas, con el fin de ser controladas eventualmente por el Juez y la defensa; las circunstancias en las que se puede realizar el borrado o la destrucción de dichas cintas, sobre todo tras un sobreseimiento o una absolución".
[1500] STJUE de 20 de mayo de 2003, Rechnungsof y otros v. Österreichischer Rundfunk y otros, asuntos acumulados C-465/00, C-138/01 y C-139/01, FJ 77.
[1501] Considerando 33, Directiva 95/46/CE.

que exista un apremio social real y que la medida sea proporcional con respecto al objetivo perseguido.

En primer lugar, cuando se habla de necesidad, no se hace referencia a un concepto flexible como pudiera ser el de "deseable" o "útil", sino a una verdadera necesidad social[1502]: "El adjetivo necesario, a los efectos del artículo 8, apartado 2, del CEDH, implica que esté en cuestión <<una necesidad social imperiosa>> y que la medida adoptada sea <<proporcionada a la finalidad legítima perseguida>>"[1503]. Las autoridades nacionales tienen un gran margen de apreciación a la hora de determinar si existe esta necesidad o no, sin embargo, el alcance de este margen dependerá de la naturaleza del objetivo que se pretende con la intromisión y de la naturaleza de esta injerencia[1504]. Siguiendo esta línea de interpretación la AN ha determinado el significado de lo que se ha de entender por "necesidad social imperiosa". Señala esta instancia que el límite no puede responder a criterios puramente de oportunidad sino que tiene que haber razones "suficientes, convenientes y convincentes" que justifiquen la adopción de esta medida. Además, estas razones deberán estar vinculadas necesariamente a la protección del interés general[1505].

En segundo lugar, para que la limitación del derecho fundamental sea acorde a derecho, y pueda considerarse como necesaria en una sociedad democrática, deberá ser proporcional. Basta ahora con recordar que según el TC, para ver si una medida restrictiva de un derecho fundamental respeta este principio, hay que atender a tres elementos: si la medida es idónea, es decir, si es susceptible de conseguir el objetivo propuesto; necesaria, esto es, que no exista otra medida más moderada para la consecución del fin propuesto; y proporcionada en sentido estricto, es decir, si su adopción aporta más beneficios que perjuicios[1506].

Partiendo de los parámetros que se acaban de exponer, corresponde en este momento señalar las excepciones que la normativa establece al derecho a la información.

II.4.2. Análisis del artículo 5.3. de la LOPD.

La primera excepción, y sin duda la más problemática, la establece el artículo 5.3 de la LOPD: "*no será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban".*

II.4.2.A. Estudio del contenido del artículo 5.3 LOPD y referencia a la posible contradicción entre la Directiva europea y la Ley estatal de protección de datos.

Este precepto reconoce una excepción general al el derecho a ser informado. La cuestión de fondo que se plantea es si, partiendo de la redacción de esta disposición, se puede llegar a entender que en el ámbito sanitario no será necesario que el responsable del fichero transmita al

[1502] STEDH de 22 de octubre de 1981. Caso Dudgeon. FJ 51.
[1503] STJUE de 20 de mayo de 2003, Rechnungsof y otros v. Österreichischer Rundfunk y otros, asuntos acumulados C-465/00, C-138/01 y C-139/01, FJ 83.
[1504] STEDH de 22 de octubre de 1981. Caso Dudgeon, FFJJ 58 y 59.
[1505] SAN 24 de marzo de 2004, FJ 8 y 9.
[1506] SSTC, 10 de abril del 2000, FJ. 9; 10 de julio del 2000, FJ 6; 5 de abril de 1999, FJ 7.

usuario del sistema sanitario información sobre diferentes características del tratamiento de datos que se va a llevar a cabo, si dicho usuario tiene la posibilidad de deducir claramente dicha información de la naturaleza de los datos o de las circunstancias que rodean a la recogida de datos.

Parece que la redacción de este punto en la LOPD es fruto de la trasposición de la letra de la Directiva europea. Se dice que "parece", pues si bien de una primera lectura pudiera concluirse que la redacción de ambas normas es semejante, las diferencias en el contenido son sustanciales[1507]. Lo dispuesto por la Ley estatal ya se ha trascrito. La norma europea, por su parte, señala que "*Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: (…) c) cualquier otra información tal como: -los destinatarios o las categorías de destinatarios de los datos; -el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder; -la existencia de los derechos de acceso y rectificación de los datos que le conciernen*; *en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado*"[1508].

La redacción de la norma europea no es precisamente afortunada, pues de ella se podría deducir que la obligación de informar sobre estos elementos es la excepción, mientras que la falta de información es la norma común. Llevando a cabo una interpretación acorde a una posición más garantista que la que se puede deducir de la lectura literal de dicho artículo, se puede entender que la norma europea exige que el responsable del fichero informe sobre las facultades señaladas, dependiendo de si las circunstancias en las que se produce la recogida de datos dan a entender que esa información es necesaria. Se entiende, por lo tanto, que tomando en consideración esas mismas circunstancias es posible limitar el derecho a la información sobre estos puntos. Si bien en un principio se pudiera decir que las excepciones recogidas en la Directiva y en la LOPD son equiparables, de una lectura más exhaustiva de la norma europea se deduce que no es así.

La Directiva entiende que dependiendo de las circunstancias que rodeen la recogida de los datos de carácter personal cabrá la excepción a la obligación del responsable del fichero a informar sobre los aspectos señalados. Estas circunstancias se identificarán en cada caso pero necesariamente deberán fundamentarse en bienes jurídicos de suficiente entidad. La LOPD, por su parte, considera que esta excepción al derecho a ser informado se dará, no cuando haya unas circunstancias lo suficientemente relevantes como para limitar dicho derecho a ser informado, sino cuando de esas circunstancias que rodean la recogida se deduzca el contenido citado. Como se verá, la posibilidad de deducir estos elementos de las circunstancias que rodean a la recogida de datos es prácticamente nula.

[1507] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, p. 147.
[1508] Artículo 10 Directiva 95/46/CE.

La norma interna debería haberse limitado a desarrollar el precepto de la Directiva, incluyendo, en todo caso, mayores garantías que las dispuestas en la norma europea, pero no dando una interpretación más flexible de ésta. Las Directivas fijan una regulación de una materia que supone un mínimo obligatorio al que todos los ordenamientos internos han de llegar a través del medio jurídico que estimen más oportuno[1509]. Pues bien, cabe preguntarse si, dentro de este concepto de desarrollo normativo que ha de llevar a cabo el ordenamiento interno, puede tener encaje la excepción incluida en la norma interna.

La aprobación de la Directiva tiene su fundamento en la necesidad de armonización de los diferentes ordenamientos internos[1510]. A través de la Directiva la UE lleva a cabo una regulación con la finalidad de aproximar las diferentes legislaciones de los países miembros. Necesariamente esta ordenación de la materia, en este caso referida a los datos de carácter personal, ha de ser respetada por los Estados. Siguiendo este criterio, la LOPD no puede desbordar el contenido de la norma supranacional a la hora de fijar límites a un derecho fundamental. La norma europea establece unos mínimos en la regulación del derecho comentado, y más allá de esta regulación, la Ley interna no puede establecer garantías menores a las dispuestas en la norma supranacional. No parece descabellado afirmar que esta situación puede llevar a plantear serias dudas sobre la validez de la disposición que ahora se comenta[1511].

En relación a esta cuestión, hay que tener en cuenta la exigencia de la jurisprudencia de interpretar las excepciones a los derechos fundamentales de manera restrictiva, exigencia que en el caso del derecho a la autodeterminación informativa se refuerza con la consideración expresa en la memoria explicativa del Convenio de protección de datos de 1981 de que las excepciones a este derecho se interpreten de manera estricta[1512]. Si se entiende que es obligación del Estado transponer la letra de la Directiva europea, lo que no podrá hacer, de acuerdo con el requerimiento de la citada jurisprudencia, es llevar a cabo una interpretación amplia de las excepciones que reconoce la normativa supranacional. En el caso que ahora se presenta, no está claro que el legislador estatal no haya optado por realizar una interpretación expansiva de la excepción recogida en la norma europea.

Por otro lado, y si bien es cierto que el precepto que aquí se comenta no ha tenido una aplicación extensa en la práctica, se entiende que resulta de interés subrayar algunos aspectos del contenido del mismo.

A) En primer lugar, hay que apuntar que esta disposición se aplica a los casos en que la información se recoge del propio titular de los datos y no por otra vía. Evidentemente, si el hecho típico de esta excepción es que el titular de los datos es capaz de deducir el contenido de gran

[1509] Artículo 249 Tratado de Ámsterdam. LASAGABASTER HERRARTE, *Fuentes del Derecho…*, cit., 2007, p. 265.
[1510] Artículo 100.A) Tratado constitutivo de la Comunidad Europea, actual Artículo 94 y siguientes, en la versión consolidad del Tratado constitutivo de la Comunidad Europea: **"***El Consejo adoptará por unanimidad, a propuesta de la Comisión y previa consulta al Parlamento Europeo y al Comité Económico y Social, directivas para la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros que incidan directamente en el establecimiento o funcionamiento del mercado común".*
[1511] CONDE ORTIZ, *La Protección...,* it., 2005, p. 91: en relación al art. 5.3 LOPD.
[1512] Punto 56 Memoria Explicativa del Convenio 108/1981 del Consejo de Europa, 1981; MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, p. 155

parte de la información que el responsable del fichero debería de darle, esta deducción sólo es posible si los datos se recogen del propio titular. Si los datos se recogen por una fuente distinta al titular de los mismos será difícil que este último pueda deducir nada, pues desconoce cuales son las circunstancias que rodean a la recogida de datos.

B) En segundo lugar, cabe subrayar que el contenido de esta excepción varía respecto a lo dispuesto en la anterior norma estatal reguladora de la protección de datos. La LORTAD disponía que la excepción de informar alcanzaba a todo el contenido del artículo 5.1, mientras que la Ley hoy día vigente limita la excepción a tres puntos del contenido de la información. Si antes se entendía que en base a esta excepción no había que informar al titular de los datos sobre ninguno de los puntos recogidos en el citado artículo, ahora se mantiene, en todo caso, la obligación de informar sobre la existencia del fichero o tratamiento de datos, la finalidad de la recogida y los destinatarios de la información, y la identidad y dirección del responsable del tratamiento o su representante.

Esta nueva regulación tiene plena justificación. Mantener la obligación de informar al titular de los datos sobre la finalidad que se persigue con el tratamiento de los datos y los destinatarios de la información supone asegurar o garantizar un mínimo de información, necesario en el ejercicio del derecho a la autodeterminación informativa. Así lo han reconocido también las resoluciones de la AEPD[1513], que exigen además que la información sobre la finalidad sea lo más concreta posible[1514]. De inicio, podría pensarse que en determinados casos la finalidad es un elemento deducible de las circunstancias en que se recaban los datos. Imagínese la realización de un contrato con una compañía telefónica en la que parece evidente que la finalidad del tratamiento de los datos será la ejecución de dicho contrato. Sin embargo, esta posibilidad plantea principalmente dos problemas. Primero, que la finalidad que en un inicio parece fácilmente deducible esconda otros objetivos que quizás no son tan claros. Siguiendo con el ejemplo anterior, puede suceder que los datos empleados para la ejecución del citado contrato se empleen también para la remisión de publicidad… Y segundo, hay que tener en cuenta que la facultad de deducción de cada uno responde a elementos puramente subjetivos; lo que uno puede deducir puede que otro no lo deduzca. Por ello, en un punto tan relevante como la finalidad que va a perseguir el tratamiento de los datos, queda justificado el que en todo caso haya que informar al titular de los datos.

Si realmente se comprende el derecho a la autodeterminación informativa como la capacidad de controlar los datos que conciernen a cada uno, no puede quedar resquicio alguno en la

[1513] Resolución AEPD 00451/2005, 20 julio de 2005, procedimiento AAPP/00029/2004: "El derecho a ser informado quedaría sin duda frustrado si se excluyeran los supuestos en los que los afectados conocen la captación de imágenes con una cámara situada en su puesto de trabajo o en las entradas al edificio, pero desconocen las finalidades de la misma".

[1514] Resolución AEPD, 00647/2005, 5 septiembre de 2005, procedimiento PS 00053/2005: "De su literalidad no se aprecia que exista información sobre finalidades determinadas y explícitas a las que se vinculará el tratamiento de los datos pues se limita a el término finalidad "*comercial"*, que, por su extraordinaria amplitud, según el Diccionario de la Lengua "*perteneciente al comercio y a los comerciantes",* no explicita con una determinación suficiente la información que previamente debe ser conocida por lo clientes". "Por otra parte, la referencia a "*cesión de datos a las distintas empresas del Grupo Pelayo",* es, asimismo indeterminada pues no concreta quienes van a ser los destinatarios de la información".

regulación de dicho derecho, que posibilite que se dé un tratamiento de datos sin que el titular de los mismos conozca la finalidad a la que se van a destinar. Si el conocimiento de la finalidad se dejara al albur de la facultad de deducir de cada sujeto, se correría el riesgo de vaciar de contenido el derecho a la autodeterminación informativa.

Lo mismo ocurre con la identidad y dirección del responsable del tratamiento. Se trata de información que no se puede deducir en ningún caso de las circunstancias que rodean a un tratamiento o de la naturaleza de los datos que se recaban. Una cosa es que se pueda deducir el carácter obligatorio o facultativo de la respuesta a las preguntas que se le plantean, y otra que se pueda deducir la identidad y dirección del responsable del fichero.

C) En tercer lugar, resulta necesario valorar una serie de puntos oscuros del contenido del precepto, que generan cierta inseguridad desde la perspectiva de la salvaguarda del derecho a la autodeterminación informativa. Por un lado, cabe subrayar la ambigüedad de este artículo. Las expresiones "*la naturaleza de los datos"* y *"las circunstancias en que se recaban"*, de ninguna manera se pueden considerar como claras y concretas[1515]. Su redacción genera cierta inseguridad jurídica[1516]. ¿Hasta donde puede estirarse la interpretación de este artículo para limitar el derecho a la información? La jurisprudencia ha afirmado, siguiendo lo que se ha apuntado sobre los límites a los derechos fundamentales, que la "relevancia del derecho conlleva que su exclusión requiera el mandato expreso de una norma, acogiendo una interpretación estricta, vedándose su extensión mediante artificiosas deducciones"[1517]. De la lectura del precepto no puede desprenderse que se está ante un mandato expreso que no da lugar a ambigüedades. ¿A qué se hace referencia con las expresiones "*naturaleza de los datos*" y "*circunstancias en que se recaban*"? Si la Ley no fija criterio alguno para conocer cómo puede deducirse de los citados elementos la información que se exceptúa, es difícil reconocer en la práctica cuándo se puede considerar que la deducción es posible.

Por otro lado, cabe preguntarse quién decide cuándo se dan las circunstancias necesarias para entender que la deducción es posible. De la redacción de la Ley se puede entender que es el propio responsable del fichero el que en la práctica, cuando recoja los datos de carácter personal, determinará si de la naturaleza de los datos o de las circunstancias en que los datos se

[1515] ULL PONT, *Derecho Público...,* cit., 2003, p. 126, en relación a las excepciones del artículo 5.3 LOPD: "Ninguno de los dos supuestos nos parecen aceptables, pues la afirmación de <<claramente deducibles>>, es muy genérica y subjetivamente cuestionable. Lo mismo podemos decir sobre <<las circunstancias en que se recaban>>. ¿Qué circunstancias son esas? A nuestro parecer, no hay claridad de deducción, en general, ni circunstancias, que legitimen omitir parte de la información requerida en el art. 5.1.
Tal excepción dada la inconcreción de los conceptos por los que se alega permite una discrecionalidad total, que podría dejar inoperante el derecho reconocido. El principio de seguridad jurídica queda vulnerado, y por supuesto pueden quedar desprotegidos los derechos reconocidos en el art. 18.4 CE. Entendemos debe ser suprimido por inconstitucional".

[1516] LÓPEZ GARRIDO, "Aspectos de…", cit., 1994, p. 24, considera que "la excepción que en él (artículo 5.3 de la LOPD) se hace respecto de las obligaciones de información a que se refiere el apartado 1, pueden llevar por su extrema abstracción y vaguedad, a un vaciamiento de las garantías de ese apartado. Eso significaría no sólo una vulneración del artículo 18.4 , en cuanto que habría un grave peligro para la intimidad, sino también del artículo 9.3 de la Constitución, que garantiza la *seguridad jurídica*"; MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, p. 147.

[1517] SAN 15 de junio de 2001, FJ 3.

recaban, se deduce la información que se excepciona en el comentado artículo[1518]. Así, esta facultad, sólo podrá ser controlada *a posteriori* por la agencia de protección de datos correspondiente. Parece evidente que esta situación otorga a la persona que recoge los datos un alto poder de decisión, que además podrá emplear con gran discrecionalidad debido a la indeterminación de los términos[1519].

El principal punto oscuro en el precepto comentado lo constituye el hecho de que la excepción al derecho se basará en la posibilidad de "deducir" las circunstancias a las que se refieren las letras b), c) y d) del artículo 5.1.

Ya se ha dicho que el término "deducir" es problemático. Si la posibilidad de deducir cierta información sobre los parámetros que van a rodear el tratamiento que se va a dar a unos datos que se recaban, hace que sea innecesario que el responsable del fichero informe al titular sobre los mismos, parece justificado exigir, para que dicha excepción sea aplicable, que esa deducción sea clara. La deducción no podrá derivar de una mera presunción o suposición, sino de hechos concretos y reconocibles que reflejen que existe cierta seguridad en que la deducción resulta objetivamente factible[1520].

Hay que tener en cuenta que la posibilidad de deducir determinados elementos sobre los que, en principio, se ha de informar es mínima. Se podría asumir que fundamentándose en el sentido común, y se habla de sentido común, pues habría que preguntarse qué capacidad se le supone al responsable del fichero para deducir los aspectos recogidos en la excepción que se comenta[1521], en determinadas situaciones son deducibles el carácter obligatorio o facultativo de la respuesta y las consecuencias de la obtención de los datos o la negativa a suministrarlos[1522]. No obstante, de ninguna manera se puede comprender cómo se puede deducir de esos elementos la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición[1523].

Ciertamente, es difícil imaginar unas circunstancias de las que se pueda deducir claramente la posibilidad de ejercer los derechos de acceso, cancelación, rectificación y oposición[1524]. La posibilidad de limitar el derecho a ser informado sobre estos elementos basándose en la capacidad de deducción del titular de los datos ha de ser criticada. El derecho a ser informado constituye un vehículo necesario para poder ejercer los derechos de acceso, cancelación, rectificación u oposición, pues es complicado ejercer dichos derechos cuando no se conoce su existencia[1525]. Así, puede comprenderse fácilmente que la falta de información sobre estos elementos anula en la práctica la posibilidad de ejercerlos, constituyendo una verdadera

[1518] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, p. 149-151.
[1519] LÓPEZ MUÑIZ GOÑI, "La Ley...", cit, 1994, p.107.
[1520] FREIXAS GUTIÉRREZ, *La Protección...*, cit., 2001, p. 162.
[1521] HERRÁN ORTIZ, *La Violación...*, cit., 1998, p. 154, se pregunta si representa la recogida en el artículo 5.3 de la LOPD (antes LORTAD), "una excepción que permite la generalización para todo tipo de personal, o habrá que tener en cuenta las circunstancias y capacidad intelectual de cada persona".
[1522] MURILLO DE LA CUEVA, *Informática y Protección...*, cit., 1993, p. 63.
[1523] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 106; LEGALIA, *La Protección...*, cit., 2002, p. 93.
[1524] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 92.
[1525] HERRÁN ORTIZ, *El Derecho...,* cit., 2002, p. 150; GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 251.

excepción a los mismos. Se entiende que esta forma de encubrir una excepción al ejercicio de estos derechos no puede tener cabida en el ordenamiento, pues crea una situación de inseguridad jurídica difícil de salvar[1526].

De todo lo dicho puede concluirse que la redacción del artículo 5.3 de la LOPD no es ni mucho menos acertada. Genera dudas que incluso podrían llevar a plantear su inconstitucionalidad[1527]. La indeterminación de sus términos[1528] deja un amplio margen a la discrecionalidad del responsable del fichero[1529], lo cual tiene dudoso encaje con el principio de seguridad jurídica recogido en el 9.3 de la CE. Por otro lado, la excepción a la obligación de informar que se recoge en el citado artículo puede llegar a encubrir una excepción a los derechos de acceso, rectificación, oposición y cancelación, lo que atenta contra el derecho fundamental a la autodeterminación informativa[1530], pues las excepciones a un derecho fundamental han de ser antes de nada claras y precisas, claridad y precisión que no se dan en este caso.

Ante la vigencia del artículo comentado de la Ley sólo cabe llevar a cabo una interpretación especialmente restrictiva del mismo, de tal forma que su aplicación no suponga un trastorno para la salvaguarda del derecho a la autodeterminación informativa de los ciudadanos[1531]. Así lo entendió también la propia AEPD cuando todavía estaba en vigor la Ley anterior[1532].

II.4.2.B. La dificultad de aplicar la excepción en el ámbito sanitario.

Atendiendo a las consideraciones realizadas se tratará de aplicar el límite que se comenta a la realidad sanitaria. En general, lo que se plantea es si en este ámbito, cuando los datos se recogen del propio titular, de las circunstancias en que se recaban dichos datos o de la naturaleza de los mismos es posible deducir la información que en principio el responsable del fichero ha de transmitir al titular de los datos. En particular, la cuestión principal a analizar no es otra que la disyuntiva ya apuntada anteriormente: compatibilizar la necesidad de agilizar o simplificar procedimientos en la realización de diferentes tareas y el respeto del derecho a la autodeterminación informativa[1533].

Lo cierto es que no se han producido muchos comentarios en torno a la aplicación de la disposición en el ámbito sanitario. Ni la normativa, ni la jurisprudencia, ni la doctrina se han

[1526] STC de 30 de noviembre de 2000, FJ 15: "la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica".
[1527] GAY FUENTES, *Intimidad y Tratamiento...,* cit., 1995, p. 86.
[1528] GARCÍA-BERRIO HERNÁNDEZ, *Informática y Libertades...*, cit., 2003, p. 191.
[1529] LÓPEZ GARRIDO, "Aspectos de Inconstitucionalidad...", cit., 1994, pp. 24 y 25.
[1530] ULL PONT, *Derecho Público...*, cit., 2000, p. 121; LÓPEZ GARRIDO, "Aspectos de Inconstitucionalidad...", 1994, cit., p. 24.
[1531] MURILLO DE LA CUEVA, *Informática y Protección...*, cit., 1993, p. 63.
[1532] Memoria de 1995, AEPD, exigía que la interpretación del artículo 5.3 fuera "notablemente restrictiva", ya que "un consentimiento consciente e informado por parte del afectado (...) se gesta en la recogida de los datos".
[1533] CARDONA RUBERT, *Informática y Contrato...,* cit., 1999, p. 120.

pronunciado expresamente sobre esta cuestión con profundidad suficiente[1534]. En la ya citada Circular del INSALUD, y en concreto en su regulación del derecho a ser informado, no se recoge esta excepción. Tampoco en la Recomendación del Consejo de Europa sobre datos médicos. La única referencia a esta excepción se encuentra en la memoria explicativa de dicha recomendación[1535]. En este documento se reconoce, al igual que lo hace la LOPD, la posibilidad de que no se informe al titular de los datos sobre alguno de los puntos sobre los que en principio se debería informar, cuando se entienda que dicha información es obvia para el paciente debido al contexto en el que se recogen los datos. Sin embargo, el contenido de la memoria que se acaba de citar no es exactamente el mismo que recoge la LOPD. Por un lado, la primera reconoce la posibilidad de exceptuar cualquiera de los puntos sobre los que en principio habría que informar, mientras que la LOPD limita esa posibilidad a unos puntos determinados. Por otro lado, la memoria explicativa de la Recomendación del Consejo de Europa entiende que la deducción deberá fundamentarse únicamente en el contexto en el que se produce la recogida de datos, mientras que en la Ley estatal la deducción deberá vincularse con las circunstancias que rodean a dicha recogida y a la naturaleza de los datos que se recaban. En cualquier caso, en ambos textos el espíritu de la excepción es el mismo.

El reconocimiento de esta excepción plantea una posibilidad que en el ámbito sanitario se podría ver con buenos ojos. La rapidez es un valor muy importante en el ejercicio de la profesión sanitaria. La relevancia de la finalidad de salvaguardar la salud de las personas requiere que se facilite en todo lo posible la labor de los profesionales. En este sentido, la obligación de informar a los pacientes sobre los parámetros que van a rodear al tratamiento de los datos de cada usuario, podría suponer una carga o un procedimiento añadido a las tareas estrictamente sanitarias. En casos en que la asistencia ha de ser inmediata, como las urgencias por ejemplo, esta circunstancia se ve claramente.

Teniendo en cuenta esta idea, la excepción al derecho a ser informado que ahora se comenta puede entenderse como una posibilidad de facilitar el trabajo de los profesionales sanitarios. Se podría interpretar que esta regulación es positiva, pues su amplitud o flexibilidad da pie a que en ella puedan incluirse situaciones de muy diverso tipo. No obstante, teniendo en cuenta lo que se ha dicho sobre los problemas que plantea el contenido del artículo 5.3 LOPD, no puede considerarse que una interpretación amplia de esta excepción esté justificada por el hecho de que facilita la actividad sanitaria.

Estando de acuerdo en que el llevar a cabo la obligación de informar de una forma especialmente rigurosa puede suponer un obstáculo en la realización de la labor profesional sanitaria, la solución no puede venir por la vía de crear excepciones de dudoso encaje

[1534] SAN 15 de junio de 2001, FJ 3, en la que se niega la aplicabilidad del artículo 5.3 LOPD a un supuesto en que se recaban datos sanitarios para incluirlos en un fichero cuyo responsable es un órgano de un centro sanitario. Sin embargo, no se realiza un estudio global sobre la conveniencia o no de emplear este precepto en el ámbito sanitario.

[1535] Punto 115 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: "*The drafters of the recommendation also acknowledged that on some occasions the data subject may not have to be told some or all of the elements referred to in Principle 5.1., either because these elements are obvious to him/her from the context in which the medical data are collected, without the need for further explanation, or because he/she has already been properly informed of these elements on a previous occasion".*

constitucional, sino por la determinación de vías más flexibles de poder llevar a cabo dicha información. Habrá que ver si la aplicación del contenido del artículo 5.3 LOPD en el ámbito sanitario es posible. Parte de la doctrina ha considerado aplicable la excepción en este sector[1536], llegando a afirmar que incluso la información sobre la finalidad puede exceptuarse por ser deducible[1537]. También la jurisprudencia ha tomado en alguna ocasión puntual esta posición[1538]. Esta postura es, sin embargo, discutible.

En primer lugar, la posibilidad de exceptuar la información sobre la finalidad es nula debido a que no viene reconocida por la Ley. La capacidad del ciudadano medio de deducir, de la naturaleza de los datos y de las circunstancias en que estos se recaban, las finalidades a las que pueden destinarse los datos sanitarios es cuestionable. Es posible que todo usuario intuya que los datos serán empleados con la finalidad de salvaguardar su salud. Sin embargo, es menos probable que dichos usuarios tengan conciencia que sus datos pueden ser empleados con fines de investigación, de docencia, estadísticos, en procesos judiciales, etc.

En segundo lugar, la posibilidad de deducir el carácter obligatorio o facultativo de las respuestas a las preguntas que se pueden plantear al usuario y las consecuencias de la obtención de los datos o de la negativa a suministrarlos puede resultar más asumible. Podría afirmarse que la gran mayoría de los usuarios, o sus representantes en caso de necesitarlos, son capaces de comprender que, en principio, la información se otorga de manera voluntaria por el paciente. Igualmente, pueden deducir la idea de que las consecuencias de no suministrar una información completa y verdadera al profesional sanitario podrían redundar, en última instancia, en perjuicio de su salud. No obstante, y a pesar de poder considerar esta información como deducible, es conveniente recordar la especial relevancia que en este ámbito tiene una información completa y ajustada a la realidad del momento.

Por último, la posibilidad de ejercer los derechos de acceso, cancelación, rectificación y oposición no puede considerarse deducible, ni mucho menos, de la naturaleza de los datos ni de las circunstancias que rodean a la recogida de los datos. Ya se ha comentado lo polémica que resulta la excepción del artículo 5.3 de la LOPD en relación a estos derechos. Sin embargo, hay que recordar lo inoportuno que podría resultar, en el ámbito que aquí se trata, la aplicación de esta excepción debido a la relevancia que en el ámbito sanitario tienen estas facultades[1539]. Los derechos de acceso, de rectificación y de cancelación, particularmente, son de especial significación para el mantenimiento de la calidad de los datos. A su vez, ya se ha señalado lo relevante que resulta contar en el ámbito sanitario con una información de calidad, completa y actualizada. De esta manera, no informar sobre las facultades que se comentan podría afectar negativamente al mantenimiento de la calidad de los datos, lo cual es de difícil justificación. Incluso en algún protocolo de actuación que ha reconocido la posibilidad de aplicar la excepción del 5.3 de la LOPD en el ámbito sanitario se rechaza la posibilidad de dejar de informar sobre la

[1536] ALMUZARA ALMAIDA, *Estudio práctico...,* cit., 2007, p. 353; SÁNCHEZ CARO y ABELLÁN, *Datos de Salud...,* cit., 2004, p. 58.
[1537] TRONCOSO REIGADA, *Guía de Protección...,* cit., 2004, p. 30.
[1538] SAN 15 de junio de 2001, FJ 4. EGUSQUIZA BALMASEDA, *La Protección de datos…,* cit., 2009, p. 68.
[1539] SÁNCHEZ CARAZO, *La intimidad...,* cit., 2000, p. 137.

existencia de estas facultades[1540]. En esta línea, también informes jurídicos realizados para el sistema sanitario vasco subrayan la dificultad que plantea la aplicación del precepto que ahora se trata[1541].

En general, por lo tanto, si bien la aplicación de la disposición estudiada podría traer una mayor eficiencia desde la perspectiva de la actividad sanitaria, la posibilidad de emplear la excepción citada en este ámbito es, después de todo, mínima. La aplicación del principio de proporcionalidad ha de traer un equilibrio entre los diferentes bienes jurídicos en juego. Como se ha visto, una interpretación flexible de la normativa hace posible que la obligación de informar pueda hacerse efectiva sin afectar de manera negativa el derecho a la salud.

II.4.3. Análisis del artículo 5.5 de la LOPD.

Más allá de la excepción que se acaba de analizar, la LOPD reconoce otro grupo de límites para el derecho a la información en el artículo 5.5: "*No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.*

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prosprección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten". Esta disposición, a primera vista, supone simplemente la transposición de lo que dicta la Directiva europea[1542]. No obstante, como se verá, este ejercicio de integración de la norma comunitaria en el ordenamiento estatal plantea más de un problema.

II.4.3.A. Breve referencia a los diferentes supuestos que recoge el artículo 5.5 LOPD.

II.4.3.A.a. Aspectos generales.

Antes de nada, es de advertir que el precepto que se analiza, con la remisión que hace al "*apartado anterior*", se vincula directamente con el artículo 5.4 y se refiere a los supuestos en que los datos no son recogidos directamente del titular de los mismos. Las excepciones que se

[1540] Punto 8.1 Código Tipo de la Agrupación Catalana de Establecimientos Sanitarios, inscrito el 28 de diciembre de 2001. "al concurrir la circunstancia eximente prevista en la Ley (artículo 5.3 de la LOPD), tanto en la recogida de datos personales relativos a la salud de los pacientes de los centros o establecimientos sanitarios asociados, como en la recogida de datos personales relativos a la gestión del personal laboral o facultativo de aquellos, se obviara la información mencionada en las letras b) y c)".

[1541] Informe sobre adecuación de determinados aspectos de la Ley Orgánica de Protección de Datos de Carácter Personal al Proyecto Osabide, 6 mayo 2002.

[1542] Artículo 11.2 Directiva 95/46/CE: "*Las disposiciones del apartado 1 no se aplicarán, en particular para el tratamiento con fines estadísticos o de investigación histórica o científica, cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o el registro o la comunicación a un tercero estén expresamente prescritos por ley. En tales casos, los Estados miembros establecerán las garantías apropiadas".*

establecen sólo podrán aplicarse, por lo tanto, cuando los datos son recabados de fuente distinta a su titular. Si el artículo 5.3 concernía a los casos en que los datos son recogidos del titular, el que ahora se va a estudiar se refiere a los supuestos en que se recaban de fuente distinta a la citada, fundamentalmente a través de una cesión o de fuentes accesibles al público.

Teniendo en cuenta precisamente los supuestos a los que se aplica el precepto a analizar, llama la atención la cantidad de excepciones que se prevén en este caso al derecho a ser informado. Resulta contradictorio el hecho de que para los supuestos en que los datos no son recabados del propio titular se reconozcan unas limitaciones tan amplias[1543]. Hay que tener en cuenta que, en la medida en que no se recogen del propio titular, la única vía por la que éste puede tener conocimiento del tratamiento de datos es la información que el responsable del fichero le ha de dar. Si esta información no se facilita, el derecho a la autodeterminación informativa queda prácticamente vacío de contenido.

La importancia de la información cuando los datos no son recogidos del titular queda reflejada en la propia Ley. Cuando esta norma sanciona el incumplimiento del deber de informar lleva a cabo una diferente calificación según se trate del incumplimiento del artículo 5.3 de la Ley o del 5.4. Si el incumplimiento se da cuando los datos han sido recabados del propio titular, será calificado simplemente como infracción leve[1544]. Por el contrario, si el incumplimiento se da cuando los datos son recogidos de fuente distinta al titular, será calificado como grave[1545]. La lógica de esta distinción es la apuntada: cuando los datos se recaban de fuentes distintas al titular, la información se convierte en fundamental para la pervivencia de un mínimo control del afectado sobre la información que le concierne. Partiendo, precisamente de este argumento, llama la atención que para los casos en que los datos son recabados de fuente distinta al titular las excepciones sean mayores que cuando la información se recaba del propio titular.

En relación al contenido del artículo 5.5 LOPD, cabe hacer un estudio comparativo entre lo que dispone la norma estatal y lo que señala la Directiva europea. Las excepciones del artículo que se comenta no venían recogidas en la anterior Ley estatal de protección de datos y se entiende que su incorporación a la Ley actual deriva directamente de la transposición de la Directiva europea. No está claro sin embargo que dicha incorporación se haya llevado a cabo de manera correcta.

La LOPD reconoce en este artículo tres supuestos diferentes en los que el derecho a la información puede quedar exceptuado: 1) que la excepción esté prevista en una Ley, 2) que la información exija esfuerzos desproporcionados según la agencia de protección de datos pertinente, y 3) que el tratamiento se dirija a cumplir fines científicos, estadísticos o históricos. Según parte de la doctrina[1546], de la lectura de la norma europea se deduce que la excepción es única: se exceptúa el derecho a la información cuando el tratamiento de datos tiene fines

[1543] PRIETO GUTIÉRREZ, "La Directiva...", cit., 1998, p. 1.108.
[1544] Artículo 44.2.d) LOPD: "*Son infracciones leves: d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley*".
[1545] Artículo 44.3.l) LOPD: "*Son infracciones graves: l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado"*.
[1546] HERRÁN ORTIZ, *El Derecho...,* cit., 2002, p. 219.

estadísticos o de investigación y, para el cumplimiento de dichos fines, el ejercicio de la información resulta imposible o requiere un esfuerzo desproporcionado o dicho tratamiento está previsto por la Ley.

Ciertamente, no es sencillo interpretar la letra de la norma comunitaria. En todo caso, si bien podría plantearse cierta divergencia en lo dispuesto por las diferentes normas, se entiende aquí que ambas son perfectamente compatibles si se realiza la interpretación adecuada.

II.4.3.A.b. Excepción al derecho a ser informado cuando una Ley lo prevea.

El primer supuesto exceptuado se refiere a cuando una Ley prevea la excepción. Este límite tiene soporte en una interpretación sistemática de la LOPD. Esta norma prevé expresamente la posibilidad de que una Ley establezca excepciones al consentimiento[1547]. Siendo esto así parece lógico pensar que, de la misma forma que con el derecho a consentir, el legislador puede identificar excepciones al derecho a la información. Se trata de un supuesto común, que al analizar el derecho a otorgar el consentimiento se estudiará con mayor detenimiento, pues plantea el problema de determinar qué rango habrá de tener la Ley que recoja dicha limitación.

Sin embargo, para que esta excepción sea aplicable se han de fijar ciertos matices. En primer lugar, se interpreta que para dar validez a este limite en un caso concreto no bastará con que una Ley prevea un tratamiento de datos. El hecho de que una Ley reconozca la posibilidad de llevar a cabo una manipulación de datos no significa que el derecho a la información queda automáticamente exceptuado. Según la interpretación realizada por las agencias de protección de datos es necesario que la norma disponga expresamente que el tratamiento de datos es necesario[1548]. La obligatoriedad de emplear la información hace que se exceptúe el derecho a ser informado.

Este criterio ha de ser interpretado de la forma más restrictiva posible. Si bien es cierto que el derecho a consentir un tratamiento puede venir exceptuado porque el legislador considere que una manipulación de datos es necesaria, la interpretación a realizar con el derecho a ser informado ha de ser diferente, pues este derecho constituye el último recurso del titular de los

[1547] Artículo 6.1 LOPD.

[1548] Informe jurídico 60/2004, AEPD, sobre Exención del deber de Informar cuando el Tratamiento o la Cesión están expresamente previstos en una Ley: "una interpretación coherente del artículo 5.5 de la Ley Orgánica 15/1999, a la vista de lo establecido en la Directiva 95/46/CE de que trae causa, implica que el deber de información al afectado quedará exceptuado en los supuestos en que el tratamiento o cesión de datos venga expresamente regulado en una norma con rango de Ley".
"(…) es preciso aclarar que la aplicación de la excepción del artículo 5.5 a la que venimos refiriéndonos en este caso será aplicable a supuestos como el aquí analizado, en que el tratamiento o cesión de los datos de carácter personal aparece recogido expresamente en una norma con rango de Ley, pero no a aquellos supuestos en que la Ley "autorice" o "habilite" la cesión de los datos, pero no la recoja de modo expreso y taxativo en su articulado".
Hace referencia este informe a una resolución de la propia AEPD: "El artículo 5.5 también exceptúa de la obligación de informar cuando expresamente una Ley lo prevea. De la interpretación literal del artículo resultaría que la obligación de informar debe estar expresamente exceptuada en una Ley para que se cumplan las condiciones previstas en este supuesto. Sin embargo, la Directiva 95/46/CE, que ha sido traspuesta por la Ley 15/1999, en su artículo 11.2 especifica que no existe deber de informar en particular para el tratamiento (...) o el registro o comunicación a un tercero estés expresamente prescritos por ley, por lo que ha de interpretarse este supuesto de exclusión en los términos previstos en la Directiva, quedando excluida la obligación de informar cuando la cesión de datos estén expresamente en una Ley". En el mismo sentido Dictamen AVPD CN10-016, 9 de agosto de 2010.

datos para conocer lo que ocurre con la información que le concierne. En relación al consentimiento, el legislador puede entender que para cumplir determinados fines es necesario prescindir de la autorización del titular. En estos casos, si no se exceptuara el consentimiento el tratamiento de unos datos se sometería a la voluntad de su titular. En el caso del derecho a ser informado no ocurre lo mismo. Informar a un sujeto sobre los parámetros en los que se manipulará la información que le concierne no impide que un tratamiento de datos se lleve a cabo. Más allá de que el legislador considere que la manipulación es necesaria para conseguir un fin determinado, la información al titular no evitará que dicho tratamiento se lleve a cabo. Es por ello que la excepción que ahora se estudia ha de ser interpretada de manera especialmente estricta.

En segundo lugar, habrá de tenerse en cuenta, que la Ley que fije la excepción al derecho a ser informado deberá cumplir con los requisitos que exige el TEDH para las normas que disponen límites a los derechos fundamentales. Como se ha visto más arriba, en términos generales la Ley deberá ser clara y precisa, deberá fundamentar la excepción en un bien jurídico suficiente y deberá respetar el principio de proporcionalidad. En base a lo dicho, la excepción al derecho a ser informado por previsión legal se producirá cuando una Ley recoja expresamente la obligatoriedad de llevar a cabo una manipulación de datos y la información dificulte la realización de dicha manipulación.

Por lo que respecta al ámbito sanitario no se identifica ninguna Ley que reconozca expresamente la excepción de informar al titular de los datos cuando estos son recabados por fuente ajena al titular. Es más, como ya se dijera, en la ya citada Circular del INSALUD sobre la protección de datos en el ámbito sanitario se aboga por el respeto al derecho a ser informado en todo caso[1549]. De la misma forma las últimas normas que entran a regular la materia sanitaria recogen también referencias a la obligación de informar dispuesta en la LOPD[1550].

II.4.3.A.c. Excepción al derecho a ser informado cuando los datos son manipulados con fines científicos.

Si bien el límite al derecho a ser informado que se acaba de analizar no plantea mayores problemas de interpretación, no ocurre lo mismo con las otras dos excepciones que recoge la LOPD en el primer apartado del artículo 5.5, ya que cuentan con un contenido más complejo.

Se señala primero el caso de que la información se trate con fines históricos, estadísticos o científicos. Se trata de un supuesto especialmente significativo para el ámbito sanitario. Piénsese que las cesiones de datos entre centros y otras entidades con el fin de llevar a cabo estudios científicos es una actividad común. Como se ha dicho al analizar las finalidades, para la salvaguarda de la salud de las personas la investigación constituye una actividad de relevancia especial. Facilitar, por lo tanto, esta tarea es fundamental. De ahí que en cuanto a la información

[1549] Instrucción nº 9, Circular 9/97 del INSALUD.
[1550] Artículo 3.2.d) RD 1718/2010, 27 de diciembre de 2010, sobre receta Médica y Órdenes de Dispensación: "*(...) En las recetas médicas en soporte papel y en la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (...)*".

a emplear en las investigaciones, las facilidades tienen que traducirse en un acceso rápido y seguro a las fuentes de la misma. En el sector de la farmacovigilancia, por ejemplo, esta necesidad de acceder a la información sanitaria con facilidad se ha recogido incluso en la normativa que regula el sector[1551]. La agilidad en el tratamiento de la información tiene su reflejo en la excepción que ahora se comenta[1552]. Evidentemente, si se exceptuara la obligación de informar a los sujetos cuyos datos se van a emplear en la investigación ésta se realizaría con mayor agilidad. Este argumento podría servir para concluir que en todo estudio científico en que se manipulan datos recabados de fuente distinta al titular no sería necesario cumplir con la obligación de informar del artículo 5 de la LOPD[1553]. Se entiende aquí que el mero hecho de que la finalidad de un tratamiento sea la investigación no puede llevar a la aplicación automática de la excepción, tal como podría desprenderse de la Ley.

Lo cierto es que el tratamiento de datos de carácter personal con fines de investigación plantea problemas jurídico-prácticos no sólo en relación al derecho a la información, sino desde una perspectiva más general, que será analizada al hablar del consentimiento. En relación al derecho a la información se entiende que la aplicación de la excepción no puede ser automática. Por un lado hay que recordar la importancia del derecho a la información en los casos en que los datos son recabados de fuentes ajenas al titular. Y por otro no se puede olvidar que aplicándose esta excepción a los supuestos en que los datos son recabados de fuentes distintas al titular, para estos casos la Ley prevé una prórroga que puede llegar a los tres meses para el ejercicio de la información. Esta prórroga hace que la obligación de informar se pueda entender de manera más laxa: se reconoce un plazo de tiempo para que la información se lleve a cabo. La prórroga facilita la posibilidad de llevar a cabo la obligación de informar. La necesidad, otra vez, de buscar el equilibrio justo entre los bienes jurídicos en juego lleva a que la excepción que se analiza tenga que ser interpretada de manera restrictiva. Si las investigaciones pueden llevarse a cabo cumpliendo con la obligación de informar no existe motivo alguno para que esta obligación se vea

[1551] Artículo 53.2 Ley 29/2006, 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios: "*Los profesionales sanitarios tienen el deber de comunicar con celeridad a los órganos competentes en materia de farmacovigilancia de cada Comunidad Autónoma las sospechas de reacciones adversas de las que tengan conocimiento y que pudieran haber sido causadas por medicamentos*".
Artículo 3 RD 1344/2007, 11 de octubre, por el que se regula la Farmacovigilancia de Medicamentos de Uso Humano: "*fuentes de información en farmacovigilancia*": *"la información sobre los riesgos asociados a la utilización de los medicamentos puede proceder de las siguientes fuentes:*
a)Notificación espontánea de casos individuales de sospechas de reacciones adversas por parte de profesionales sanitarios.
b)Estudios post-autorización.
c)Bases de datos sanitarias informatizadas.
d)Información pre-clínica de experimentación animal
e)Información de los ensayos clínicos de un medicamento.
f)Informaciones relacionadas con la fabricación, conservación, venta, distribución, dispensación, prescripción y utilización de los medicamentos.
g)Publicaciones científicas.
h)Otras fuentes de información, como las relativas al uso incorrecto y abuso de medicamentos, o las correspondientes a errores de la medicación que puedan aportar datos relevantes para la evaluación de los beneficios y riesgos de los medicamentos.
i)Otras autoridades sanitarias y organismos sanitarios internacionales".
[1552] DE MIGUEL SÁNCHEZ, *Secreto Médico...,* cit., 2002, p. 275.
[1553] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 79.

exceptuada. Partiendo, por lo tanto, de la idea de que la aplicación de la excepción no puede ser automática, se han de determinar los casos en que puede emplearse.

La limitación deberá dirigirse a la salvaguarda de un bien jurídico de relevancia y deberá atenderse al principio de proporcionalidad, que exige para cumplir ese fin que la manipulación de datos se lleve a cabo de tal manera que cause el menor daño. En este sentido, habrá que poner todos los medios posibles para llevar a cabo la información. Y sólo se exceptuará ésta cuando sea imposible de ejecutar o requiera esfuerzos desproporcionados. El control de si se dan o no estas circunstancias puede llevarlo a cabo la agencia de protección de datos correspondiente. Teniendo en cuenta el plazo de prórroga que concede la Ley, se puede afirmar que se facilita la realización de este control.

Se concluye, por lo tanto, que puede aplicarse la excepción al derecho a la información cuando la finalidad del tratamiento es la investigación científica. Sin embargo, se entiende que la aplicación de dicha excepción debe ajustarse a los criterios indicados.

II.4.3.A.d. Excepción al derecho a ser informado cuando la información resulte imposible o exija esfuerzos desproporcionados.

La Ley recoge una tercera excepción. Se trata del supuesto en que a criterio de la agencia de protección de datos correspondiente la información resulte imposible o exija esfuerzos desproporcionados debido al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. De una primera lectura el contenido de la excepción trascrita parece razonable. No obstante es necesario realizar una serie de apuntes sobre el mismo para comprender su aplicabilidad en el ámbito sanitario.

En principio la excepción se aplicará cuando se dé alguna de las circunstancias citadas. Si bien esto es así, no se puede olvidar que este límite al derecho a ser informado, como todos los demás, deberá tener en cuenta, más allá de esas circunstancias, el bien jurídico que se pretende proteger con el tratamiento de los datos. La agencia correspondiente deberá atender, a la hora de determinar si la excepción es aplicable, al interés que se pretende satisfacer con dicha limitación. Se ha comentado en diferentes ocasiones que el límite a un derecho fundamental debe estar fundado en un bien jurídico de relevancia suficiente. No es lo mismo que la información sea imposible o exija esfuerzos desproporcionados cuando la finalidad sea propagandística o sea la salvaguarda de la salud de las personas.

La aplicación de la excepción se producirá cuando concurran estos elementos. No obstante, el respeto del principio de proporcionalidad lleva necesariamente a realizar una interpretación flexible del límite que se comenta. En beneficio de este principio, cuando se den los requisitos para que la excepción pueda ser aplicada, la solución no siempre será la asunción o no del límite al derecho a la información. Habrá ocasiones en que se reconocerán soluciones intermedias que posibiliten la ejecución de la información de una manera más laxa. En algún caso la propia AEPD ha entendido que son válidas las formas de informar que en un principio podrían parecer

contrarias a la Ley, debido a que son la única alternativa a la aplicación directa de la excepción, así es el caso de la información a través de publicaciones en prensa[1554].

Desde un punto de vista sustantivo el contenido de este precepto podría plantear alguna duda debido a la indeterminación de los conceptos que maneja. Algunos autores han puesto de manifiesto que no se establece en la Ley cuándo se entenderá que, atendiendo a los criterios de cantidad de interesados, antigüedad de datos o medidas compensatorias, se está ante un esfuerzo desproporcionado[1555]. Se interpreta aquí que la Ley establece criterios lo suficientemente claros. Hay que tener en cuenta que en un ámbito como el que se está tratando, en el que las nuevas tecnologías juegan un papel fundamental, establecer criterios más estrictos o cerrados de lo que se entiende por desproporcionado puede dejar el contenido de la norma obsoleto. Y es que lo que hoy se entiende como desproporcionado puede no serlo dentro de unos años debido a los avances de las TIC, que abren las puertas a nuevas posibilidades de tratamiento de datos. Así, ha de considerarse correcto el contenido de esta disposición. En todo caso, es cierto que hubiera sido de ayuda que la Ley hubiera recogido una lista abierta de supuestos en que se entiende que concurre un esfuerzo desproporcionado.

La consideración de que un esfuerzo es o no desproporcionado ha de hacerla la APD, la estatal o la autonómica, principal garante del derecho a la autodeterminación informativa. Ello constituye una garantía para la salvaguarda del derecho, pues no queda a discreción del responsable del fichero la comprensión o no del esfuerzo como desproporcionado. Se entiende, según la redacción de la LOPD, que el control que ha de realizar la APD pertinente sobre la cualidad del esfuerzo es un control previo al tratamiento de los datos.

La Ley no señala nada acerca del procedimiento que en la agencia correspondiente ha de seguirse para adoptar la resolución oportuna. El nuevo reglamento de desarrollo de la Ley, siguiendo las indicaciones que la agencia estatal había ido dando en diferentes resoluciones e informes, aclara ciertos aspectos del procedimiento. La decisión sobre la pertinencia o no de la excepción se resolverá a través de un acto administrativo que deberá en todo caso seguir el procedimiento marcado por la LPAC, si bien deberán tenerse en cuenta algunas particularidades[1556]. El control no comienza con una denuncia del titular de los datos sino con una solicitud del responsable del fichero que pretende emplear el precepto que se comenta como argumento para no informar al titular o titulares de los datos. La solicitud debe contener, además de los requisitos comunes[1557], la identificación del tratamiento que se pretende, la motivación de las causas que le llevan a entender que la información es imposible o exige un esfuerzo

[1554] Resolución AEPD PR/00001/2007, 17 de enero 2007: "En el supuesto presente cabe apreciar que cumplir con el principio de información respecto a los 30.000 registros incluidos en sus ficheros, supone un esfuerzo desproporcionado ya que, en muchos casos, se desconoce la actual propiedad de las localizaciones.
Ante tal situación, la sociedad Discovery 2 Localizaciones, S.L. ha expuesto que cumpliría con la obligación de informar a los propietarios de las localizaciones, cuyos datos personales estuvieran en sus ficheros, informando al contactar con ellos cuando su propiedad fuera elegida para un rodaje y, además, mediante la publicación de la información requerida por el artículo 5.1 de la LOPD en el periódico "*El Mundo*""
"(...) ambas medidas propuestas (...) se consideran suficientes (...)".
[1555] GUERRERO PICÓ, *El Impacto...,* cit. 2006, p. 255.
[1556] GUERRERO PICÓ, *El Impacto...,* cit. 2006, p. 255-256.
[1557] Artículo 70 LPAC.

desproporcionado, la indicación de las medidas compensatorias que adoptará en caso de que se le exonere de la obligación de informar, y la fijación de una cláusula informativa que mediante su difusión pueda compensar la falta de información[1558]. Estas medidas compensatorias pueden completarse con otras que la agencia estime oportunas[1559]. El plazo para resolver el procedimiento es de seis meses y el silencio, en caso de que en dicho plazo la agencia no dé respuesta alguna, es positivo, de tal forma que el responsable puede entender su solicitud como estimada[1560].

La excepción que se plantea se aplica a los casos en que la información es recabada de fuente distinta del titular de los datos. Para estos supuestos la Ley fija un plazo máximo de tres meses desde que se registran los datos para hacer efectiva la información al titular de los datos. Si se ha entendido bien, hay quien ha interpretado, antes de la aprobación del reglamento de desarrollo de la LOPD, que lo conveniente sería que la agencia resolviera dentro de estos tres meses[1561]. Ciertamente podría chocar el que se otorgue un plazo de seis meses para resolver cuando el plazo para que se lleve a cabo la información es de tres meses. No obstante, se entiende aquí que no hay contradicción entre las dos regulaciones. El procedimiento administrativo es previo al comienzo del tratamiento de los datos. Así, si la resolución de la agencia es desestimatoria de la solicitud del responsable, el plazo de tres meses para informar comenzará a computarse a partir del día siguiente a la notificación de dicha resolución.

La Ley tampoco determina qué órgano de la agencia ha de resolver este procedimiento. No obstante, como señala el reglamento de desarrollo de la misma, será el Director de la agencia quien adoptará dicha decisión[1562]. Este órgano, por lo tanto, deberá "determinar si dadas las circunstancias del caso (y, en particular las previstas en la norma) la notificación implicaría un esfuerzo desproporcionado"[1563]. La notificación de la resolución se hará al responsable del fichero que instó el procedimiento. Evidentemente, no podrá hacerse efectiva esta notificación a los titulares de los datos, a pesar de ser interesados en dicho procedimiento[1564], cuando menos si el resultado es estimatorio. Si se entiende que la información sobre los parámetros que van a rodear el tratamiento de los datos es imposible o supone un ejercicio desproporcionado, parece lógico pensar que la notificación, que no es más que una forma de informar, también será imposible. Para estos casos en que la notificación resulta especialmente complicada, la LPAC prevé diferentes opciones: anuncios en el tablón de edictos, en los boletines oficiales, el empleo de medios de difusión, su publicación, etc.[1565].

La aplicación de la excepción es perfectamente aceptable siempre y cuando se cumplan las condiciones señaladas. Como se ha apuntado por parte de la doctrina, puede tener una gran utilidad en el ámbito público cuando la actividad administrativa se dirige a un gran número de

[1558] Artículo 153.2 RDLOPD.
[1559] Artículo 154 RDLOPD.
[1560] Artículo 156 RDLOPD.
[1561] VIZCAÍNO CALDERÓN, *Comentarios a...*, cit., 2001, pp. 109-110
[1562] Artículo 155 RDLOPD.
[1563] Memoria de la AEPD de 2002, p. 297.
[1564] Artículo 31.1 LPAC: "*Se consideran interesados en el procedimiento administrativo: b) Los que sin haber iniciado el procedimiento, tengan derechos que puedan resultar afectados por la decisión que en el mismo se adopte*".
[1565] Artículo 59.5 y 6, LPAC.

personas[1566], pues evita una innecesaria burocratización del sistema. Sin embargo, en la aplicación de esta excepción la agencia correspondiente deberá adoptar, siempre que se pueda y en aras del principio de proporcionalidad tantas veces citado, sistemas o vías alternativas de información que garanticen mínimamente su aplicación. En este sentido, no puede dejarse de lado que hoy día, con la incorporación de las TIC existen nuevas formas de información, ágiles y accesibles.

II.4.3.B. Aplicación del precepto en el ámbito sanitario.

Las excepciones que se reconocen en el artículo 5.5 LOPD pueden tener su aplicación en el ámbito sanitario. Si bien, la mayoría de los datos que se manipulan se recaban directamente del titular, en algunos casos se recogen de terceras personas, familiares, o a partir de cesiones de otras administraciones o entidades, por ejemplo, dedicadas a la investigación. En estos casos, el cesionario no recibe los datos directamente de su titular por lo que podría plantearse la aplicación de las excepciones ahora apuntadas. No hay que olvidar que si se aplica este límite, el resultado será que los datos serán transmitidos a un tercero sin que el titular de los mismos conozca la información sobre la existencia y finalidad del fichero, la facultad de ejercer los derechos de acceso, cancelación, rectificación y oposición, y la identidad y dirección del responsable del tratamiento.

A) Respecto a la posibilidad de que una Ley prevea expresamente la excepción al derecho a ser informado ya se ha dicho, que en el ámbito sanitario se desconoce la existencia de norma alguna con dicha previsión expresa. Es más, como se ha podido ver, protocolos de actuación de diferentes centros sanitarios, que tratan de aplicar la regulación sobre la protección de datos a las características particulares de dichos centros reconocen, *a priori*, la vigencia del derecho a ser informado.

B) La segunda excepción hacía referencia al supuesto en que la manipulación de datos se dirige a la realización de investigaciones históricas o científicas o estudios estadísticos. Este supuesto tiene plena aplicación en el ámbito sanitario. Se han analizado suficientemente las características que este tipo de operación ha de guardar para que la excepción que ahora se plantea le sea aplicada. Basta con señalar que la mera alegación de que la finalidad del tratamiento de datos es la investigación no exceptúa automáticamente el deber de informar. Es necesario que además se den otras circunstancias. En todo caso, la regulación más reciente en materia de investigación científica reconoce sin ambages el derecho del paciente a ser informado sobre las condiciones en que sus datos de carácter personal van a ser manipulados en dicho estudio[1567]. Es más, esta regulación entra a concretar los aspectos sobre los que deberá informar el responsable del fichero ampliando el contenido que reconoce la LOPD[1568]. Se puede concluir, por lo tanto, que en la normativa dedicada a regular los parámetros entre los que se han de desarrollar las investigaciones, lejos de excepcionar la obligación de informar, se exige expresamente su cumplimiento.

[1566] GUICHOT, *Datos Personales...,* cit., 2005, p. 389-391.
[1567] Artículo 47 Ley 14/2007, 3 de julio, de Investigación Biomédica.
[1568] Artículos 15, 47 y 59 Ley 14/2007, 3 de julio, de Investigación Biomédica.

C) La última excepción que recoge la Ley puede tener también cabida en el sector sanitario. Puede resultar que en operaciones concretas el responsable del fichero se encuentre ante una situación que haga imposible o muy difícil la información a los implicados en la operación.

Hay que tener en cuenta que la actividad sanitaria se dirige muchas veces a colectivos especialmente amplios: tercera edad, niños, mujeres, afectados por una enfermedad determinada, etc. Puede darse la circunstancia de que los datos relativos a estos colectivos no hayan sido recabados directamente de los titulares. En este supuesto, si el número de individuos a los que habría de informar es especialmente elevado podría plantearse la posibilidad de aplicar la excepción que se comenta. No obstante, atendiendo a los recursos con que cuentan actualmente los sistemas sanitarios públicos no parece defendible, en términos generales, que el número de interesados imposibilite la realización efectiva de la obligación de informar. Ya se ha dicho que la forma de informar a los usuarios puede ser variada, a saber: emisión de folletos, información previa al tratamiento a través del personal auxiliar, utilización de las nuevas tecnologías.

Se podría plantear también la posibilidad de aplicar la excepción debido a la antigüedad de los datos. Es sabido que la relación entre la Administración sanitaria y los usuarios es de larga duración y que en ocasiones las historias clínicas pueden contener información de muchos años de antigüedad. Es posible que entre esta información desfasada se encuentren datos sobre el domicilio, teléfono, etc, que hicieran imposible la comunicación o la información[1569]. Lo cierto es que la antigüedad de los datos en el ámbito sanitario no debería resultar un problema, habida cuenta de que en este área, en principio, la actualización de los datos es un ejercicio particularmente controlado debido a su importancia. Esto hace que a la hora de llevar a cabo la información no deba ser tan dificultoso localizar al titular de los datos para transmitirle todo lo relativo al tratamiento de los datos.

II.4.4. Análisis del artículo 24.1 de la LOPD y otras excepciones.

Las últimas excepciones al derecho a la información que recoge la LOPD se establecen en su artículo 24.1: "*Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas*"[1570].

II.4.4.A. Perspectiva general del artículo 24.1. Crítica a la indeterminación de los conceptos que emplea.

La regulación que lleva a cabo la LOPD reproduce lo que recogía la anterior Ley orgánica de protección de datos[1571]. Esta disposición es fruto de lo que señala al respecto la Directiva

[1569] SÁNCHEZ CARAZO, *La intimidad...,* cit., 2000, p. 135.
[1570] Los aspectos subrayados han sido declarados inconstitucionales.
[1571] Artículo 22.1 LORTAD.

europea[1572], transcribiéndola sin desarrollar su contenido, lo que plantea problemas de interpretación.

En la norma estatal se otorga a este precepto rango de Ley ordinaria[1573]. Como se ha indicado en distintas ocasiones los límites a los derechos fundamentales, constituyendo desarrollo del derecho fundamental, deberían identificarse a través de leyes orgánicas. Podría entenderse que una ley ordinaria establezca esos límites, siempre que tuviera como base o fundamento una Ley orgánica. Sin embargo, en este caso no se encuentra la base adecuada con rango de Ley orgánica para el artículo que se comenta. El precepto con rango de Ley ordinaria fija por sí mismo una nueva excepción. Esta circunstancia podría llevar a cuestionar la constitucionalidad de la disposición[1574].

Es de advertir también que el artículo que se estudia ha sido especialmente polémico, llegando a declararse parte del mismo (los apartados subrayados) inconstitucional por atentar contra el núcleo esencial del derecho a la autodeterminación informativa. No corresponde en este momento hacer un análisis exhaustivo de lo que el TC declaró respecto a este artículo[1575]. Basta con constatar que las excepciones al derecho a ser informado que se recogen en la redacción actual se reducen a los casos en que la información afecte a la Defensa Nacional, la seguridad pública y la persecución de infracciones penales. En una primera lectura las excepciones citadas parecen plenamente justificadas. Sin embargo, analizándolas de manera individualizada plantean problemas, fundamentalmente la falta de claridad y precisión.

[1572] Artículo 13.1 Directiva 95/46/CE: "*Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguarda de:*
a) la seguridad del Estado;
b) la defensa;
c) la seguridad pública;
d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas;
e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales;
f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e);
g) la protección del interesado o de los derechos y libertades de otras personas."

[1573] Disposición final 2ª LOPD; "*Los títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria*".

[1574] GUICHOT, *Datos Personales...,* cit. 2005, pp. 150-151.

[1575] STC de 30 de noviembre del 2000, FFJJ 17 y 18: "el empleo por la LOPD en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que (...) permite reconducir a las mismas prácticamente toda actividad administrativa".
Con respecto a la otra excepción basada en la "persecución de infracciones administrativas", el TC concluyó diciendo que el "interés público en sancionar infracciones administrativas no resulta, en efecto, suficiente (...) la posibilidad de que, con arreglo al art. 24.1 LOPD, la administración pueda sustraer al interesado información relativa al fichero y sus datos según dispone el art. 5.1 y 2 LOPD, invocando los perjuicios que semejante información pueda acarrear a la persecución de una infracción administrativa, supone una grave restricción de los derechos a la intimidad y a la protección de datos carente de todo fundamento constitucional".

A) En primer lugar la disposición recoge la posibilidad de exceptuar el derecho a ser informado cuando la finalidad del tratamiento de datos es la persecución de infracciones penales. En principio este precepto no parece plantear excesivos problemas, porque la expresión "persecución de infracciones penales" constituye una realidad aparentemente bien definida, y porque es comprensible que dicha finalidad pueda exceptuar el derecho a ser informado. Hay que tener en cuenta que en la persecución de estas infracciones el tratamiento de datos de diferentes personas puede constituir un instrumento necesario[1576]. El hecho de que una persona conozca que sus datos están siendo empleados en una investigación concreta puede interrumpir u obstruir dicha investigación. Así, el que, en casos en que la persecución de un delito está en juego no se informe al titular de los datos sobre los elementos que exige la Ley puede constituir, *a priori*, un mal asumible o necesario. Como ha señalado la doctrina, atendiendo a la Ley una persona puede ser investigada con fines policiales sin que tenga conocimiento alguno de ello[1577].

No obstante, a pesar de partir de una primera valoración positiva del precepto, hay que hacer algunas precisiones críticas. El artículo dispone que la excepción al derecho será aplicable cuando la información "afecte" a la persecución de una infracción. Como ha señalado la doctrina, este término no es nada claro[1578]. Se podría interpretar que hay casos en que la información al titular puede no afectar, negativamente por lo menos, a la investigación. Así, *a sensu contrario*, podría entenderse que si la información no afecta negativamente a la persecución de estas infracciones permanecerá vigente la obligación de informar al titular de los datos. Ciertamente, el hecho de que la Ley no especifique cómo ha de afectar la información a la persecución del delito para que ésta no se tenga que llevar a cabo genera cierta inseguridad.

En este punto, la Directiva europea emplea un término más riguroso que el que se recoge en la norma interna. Dispone que la excepción al derecho a ser informado se aplicará cuando constituya una "medida necesaria" para cumplir los fines que justifican la limitación. Como se puede adivinar, la previsión de la norma europea remite al criterio de la proporcionalidad, que lleva a que se puedan encontrar casos en que la aplicación de la excepción a la información no constituya una medida necesaria para llevar a cabo el fin que se pretende. Por el contrario, la aplicación por parte de la norma interna del concepto "afectar" genera ciertas dudas en torno a la necesidad o no de tener que realizar ese juicio de proporcionalidad. Se entiende aquí que en todo caso, por tratarse de un límite al derecho fundamental, este ejercicio de ponderación será necesario. A esta conclusión se ha de llegar si se hace una interpretación conjunta del precepto con el resto de la Ley. En lo que concierne a la recogida y tratamiento de datos denominados sensibles por parte de las Fuerzas y Cuerpos de Seguridad, la Ley entiende que estas operaciones podrán llevarse a cabo en los casos en que sea "absolutamente necesario" para los fines de una investigación concreta[1579]. Parece indudable que el empleo de la expresión

[1576] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 33.
[1577] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, p. 108.
[1578] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, p. 84.
[1579] Artículo 22.3 LOPD. "*la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales*".

"absolutamente necesario" conlleva la necesidad de tener que llevar a cabo un juicio de ponderación, para llegar a la conclusión de que no existe alternativa a la manipulación de datos[1580]. Pues bien, esta misma interpretación se ha de hacer del precepto que ahora se analiza: la excepción a la información se llevará a cabo cuando sea necesaria para cumplir los fines citados.

Este límite plantea otras dudas que agudizan la falta de seguridad. En principio, el ámbito de aplicación del precepto parece definido. El concepto "persecución de infracciones penales" parece abrazar un amplio ámbito. Englobaría tanto faltas como delitos. Sin embargo, a la hora de concretar cuándo y cómo se puede aplicar la excepción se plantean dudas de envergadura.

La crítica principal a realizar a este contenido es que deja la puerta abierta a que las Fuerzas y Cuerpos de Seguridad puedan aplicar la excepción con un alto grado de discrecionalidad. En primer lugar, porque parece que en la investigación de las infracciones puede limitarse el derecho a ser informado de cualquier persona implicada de cualquier manera en dicha operación. No parece que la excepción haya de limitarse exclusivamente a la persona que se presume ha sido la culpable de la infracción. En segundo lugar, porque de la citada expresión no se deduce la necesidad de que estos organismos tengan cierto nivel de seguridad a la hora de calificar al titular de los datos como infractor penal. Es decir, parece que las Fuerzas y Cuerpos de Seguridad no necesitan de un determinado grado de convencimiento fundado sobre la posible participación de una persona en la comisión de una infracción para aplicar la excepción que se comenta. Y por último, porque la Ley no recoge garantía alguna para que el límite al derecho a ser informado se ejecute de manera proporcional. No prevé un sistema de control previo de la actuación de las Fuerzas y Cuerpos de Seguridad que determine si respeta las garantías mínimas de los derechos fundamentales. Esta regulación puede generar cierta controversia por cuanto que en otros ámbitos, para que las Fuerzas y Cuerpos de Seguridad puedan llevar a cabo determinadas actuaciones la autorización judicial es requisito indispensable. Es el caso del sector de las Telecomunicaciones, donde la normativa vigente exige la autorización judicial previa para que la policía pueda acceder a los datos que los operadores han de conservar a efectos de posibles investigaciones policiales[1581].

Partiendo de lo que se acaba de exponer puede concluirse que la discrecionalidad que se otorga a las Fuerzas y Cuerpos de Seguridad en el desarrollo de sus actuaciones para decidir cuándo se puede restringir el derecho a la información es especialmente amplia. Cierto es que la normativa reguladora de la actuación de las Fuerzas y Cuerpos de Seguridad exige que ésta sea

[1580] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, p. 111.

[1581] Artículo 282.bis.3 LECrim: "*Cuando las actuaciones de investigación puedan afectar a los derechos fundamentales, el agente encubierto deberá solicitar del órgano judicial competente las autorizaciones que, al respecto, establezca la Constitución y la Ley, así como cumplir las demás previsiones legales aplicables*"; Artículos 545-588 LECrim: en relación a la necesidad de que medie autorización judicial para llevar a cabo registros en lugares cerrados, libros y papeles y aperturas de la correspondencia escrita y telegráfica; Artículo 6.1 Ley 25/2007, 18 de octubre, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones: "*Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial*"; CUBERO MARCOS y ABERASTURI GORRIÑO, "Reflexiones en torno a la protección...", cit., 2008, pp. 99-100.

proporcional y prohíbe excesos arbitrarios[1582]. No obstante, el amplio margen de actuación que se otorga a estos órganos puede llevar a cuestionar si en la práctica existen garantías suficientes para que la excepción se aplique de acuerdo con el principio de proporcionalidad. Como se verá, esta misma cuestión se planteará cuando se analicen las excepciones al consentimiento en la cesión de datos sanitarios con fines policiales. También en este caso la LOPD lleva a cabo una regulación excesivamente ambigua.

En general, de la citada regulación se desprende la voluntad del legislador de dejar un amplio margen de maniobra a las Fuerzas y Cuerpos de Seguridad. Esta interpretación puede venir corroborada por las decisiones que en determinados casos han adoptado los Tribunales, dando carta blanca a actuaciones cuya legalidad puede ser puesta en duda desde la perspectiva del respeto al derecho a la información que ahora se analiza[1583].

B) En segundo lugar, además de la excepción comentada, la disposición que ahora se analiza reconoce otros dos casos en que se limita el derecho a ser informado. Se trata de los supuestos en que está en juego la defensa nacional o la seguridad pública. El empleo de estos conceptos viene obligado por el hecho de que la Directiva europea los recoge en su articulado[1584]. En este caso la norma interna simplemente se ha dedicado a transcribir el contenido de la norma europea, sin concretarlo. El texto de la LOPD no ha matizado ni desarrollado en ningún aspecto lo dispuesto por la Directiva.

El principal problema que la doctrina ha formulado con respecto a estos dos supuestos ha sido la indeterminación de los términos empleados. La defensa nacional y la seguridad pública no definen con suficiente claridad la realidad a la que se refieren[1585]. Se trata de expresiones especialmente amplias, lo cual lleva a que se puedan incluir en ellas un abanico muy extenso de actividades que no estarían sujetas a la obligación de informar al titular de los datos. Esta interpretación expansiva podría dejar sin efecto práctico el reconocimiento del derecho a la información.

La necesidad de determinar y dar contenido a estas expresiones es una exigencia que viene de lejos[1586]. Hay que tener en cuenta que a los conceptos citados en la Ley se les suman en el ordenamiento otros como los de "orden público" o "seguridad ciudadana". Ciertamente, en el ordenamiento jurídico estos términos se emplean de manera indistinta, sin que todavía hoy tengan un contenido definido que distinga a cada uno de ellos de los demás. La letra de la CE[1587], ha dado pié a diferentes interpretaciones pero difícilmente pueden extraerse conclusiones

[1582] Artículo 5.2.a) LO 2/1986, 13 de marzo, Fuerzas y Cuerpos de Seguridad.
[1583] Queda patente esta circunstancia en el conocido caso de la ilegalización de la organización política Aukera Guztiak que culmina con las STS 26 marzo de 2005, FJ. 9 y STC 31 de marzo de 2005, FJ 15. En este proceso, que ni siquiera puede considerarse como penal, el Tribunal admite la posibilidad de que las Fuerzas y Cuerpos de Seguridad manipulen datos de múltiples ciudadanos, incluso cruzando datos de carácter ideológico con información contenida en otros ficheros, sin que se lleve a cabo la obligación de informar a los titulares de los datos que se manejan.
[1584] Artículo 13.1, Directiva 95/46/CE.
[1585] DAVARA RODRÍGUEZ en APDCM, *Estudios sobre Administraciones...,* cit., 2006, pp. 177-178.
[1586] CARRO VERNÁNDEZ-VALMAYOR, "Sobre los conceptos...", cit., 1990, p. 21.
[1587] Artículo 104 CE: "*Las Fuerzas y Cuerpos de Seguridad, bajo la dependencia del Gobierno, tendrán como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana"*.

definitivas. Por su parte, la Ley Orgánica sobre Protección de Seguridad Ciudadana tampoco fija de manera clara el alcance de estos términos[1588].

Las agencias de protección de datos tampoco han entrado en sus resoluciones a delimitar expresamente el ámbito de aplicación de estos conceptos. No obstante, en alguna ocasión en que se ha aplicado la disposición que ahora se trae a colación, a la luz de lo que había fijado previamente el TC, se deja claro que la imposición de sanciones administrativas no entra en ninguno de los conceptos citados[1589]. La investigación de infracciones administrativas con la finalidad de imponer una sanción no constituye argumento suficiente para limitar el derecho del titular de los datos a ser informado.

La jurisprudencia se ha referido puntualmente a estos términos[1590]. En alguna ocasión se ha señalado que la seguridad pública consiste en el "mantenimiento de la tranquilidad u orden ciudadano"[1591]. En otro momento ha tratado de afinar algo más afirmando que la seguridad pública es la "actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano" que incluye "un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido. Dentro de este conjunto de actuaciones hay que situar, incluso de modo predominante, las específicas de las organizaciones instrumentales destinadas a este fin y, en especial, las que corresponden a las Cuerpos y Fuerzas de Seguridad, a que se refiere el art. 104 CE. Pero por relevantes que sean, esas actividades policiales, en sentido estricto, o esos servicios policiales no agotan el ámbito material de lo que hay que entender por seguridad pública en cuanto que concepto delimitador de la competencia, aun sólo ejecutiva, de los poderes públicos. Otros aspectos y otras funciones distintas de los Cuerpos y Fuerzas de Seguridad, y atribuidas a otros órganos y autoridades administrativas... componen, sin duda, aquel ámbito material"[1592]. Sin embargo, ha matizado que no todas las acciones dirigidas a la protección de las personas y bienes, ni las normas encaminadas a conseguir dicho objetivo, constituyen medidas vinculadas con la seguridad pública. Este concepto tendría un sentido más estricto, relacionándolo directamente con las funciones de los cuerpos de seguridad[1593].

En cuanto al concepto de defensa nacional, en algún caso se ha pronunciado la jurisprudencia a favor de una interpretación especialmente amplia. Según ésta, dentro de la

[1588] Artículo 1 Ley Orgánica 1/1992, 21 de febrero, sobre Protección de Seguridad Ciudadana: "*De conformidad con lo dispuesto en los artículos 149.1.29 y 104 de la Constitución corresponde al Gobierno, a través de las autoridades y de las Fuerzas y Cuerpos de Seguridad a sus órdenes, proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, crear y mantener las condiciones adecuadas a tal efecto, y remover los obstáculos que lo impidan, sin perjuicio de las facultades y deberes de otros poderes públicos".*

[1589] Resolución AEPD 00472/2005, 20 julio 2005, AAPP/00021/2004: La importancia del derecho a ser informado se puede demostrar en la práctica atendiendo a las resoluciones de la AEPD, como la que señala que la Dirección General de Tráfico ha de cumplir necesariamente con el contenido del artículo 5 cuando recaba información, por ejemplo a la hora de imponer sanciones, en el desarrollo de sus funciones, pues no se trata de supuestos que tengan que ver con la Seguridad Nacional, Seguridad Pública o persecución de infracciones penales.

[1590] AGUADO I CUDOLÁ, *Derecho de la Seguridad…,* cit., 2007, p. 47, da un interesante repaso a las más importantes sentencias que entran a otorgar contenido a este concepto.

[1591] STC 9 de junio de 2005, FJ 3. CASADO CADARSO y VILA MUNTAL, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.398.

[1592] STC 8 de junio de 1989, FJ 3.

[1593] STC 6 de mayo de 1985, FJ 2.

defensa de la nación tendrían cabida realidades muy variadas que incluso llegarían a alcanzar a la protección del sistema de seguridad social[1594].

Más allá de los matices que ha ido incluyendo la jurisprudencia, es claro el carácter indeterminado de estos conceptos. Realmente, la necesidad que fija la jurisprudencia que más arriba se ha visto, de que los límites a los derechos fundamentales aparezcan redactados de manera precisa, tiene dudoso cumplimiento en este apartado de la Ley. El problema de inseguridad que esto conlleva es evidente. La posibilidad de interpretar estos conceptos de forma especialmente amplia tiene el riesgo de que aspectos muy extensos de la realidad puedan quedar exentos del cumplimiento de la obligación del derecho a ser informado.

II.4.4.B. Posibilidad de aplicar el artículo 24.1 de la Ley en el ámbito sanitario.

Las excepciones que se acaban de comentar pueden tener su aplicación en el ámbito sanitario. El uso de datos relativos a la salud de las personas con la finalidad de prevenir o sancionar infracciones penales o de salvaguardar la defensa nacional y la seguridad pública puede ser plenamente justificable.

Se ha dicho desde un comienzo que en este ámbito el principal enfrentamiento del derecho a la autodeterminación informativa se va a dar con el derecho a salvaguardar la salud de las personas. Si bien esto es cierto, no puede dejar de apuntarse que el tratamiento de datos sanitarios puede tener una finalidad distinta. Es conocido por todos el uso de muestras de ADN para la identificación de presuntos delincuentes. Y más allá de este supuesto concreto, pueden plantearse diferentes casos en los que la defensa nacional, la seguridad pública o la persecución de infracciones penales requieren de la manipulación de datos de carácter sanitario: los resultados de un análisis médico de una persona involucrada en un accidente de tráfico, historias clínicas de individuos que se han visto afectados por una intoxicación para llevar a cabo una puesta en común de datos, etc. Es pues aceptable que los datos sanitarios puedan ser empleados con la finalidad de salvaguardar los bienes que se acaban de citar.

El cumplimiento de los objetivos comentados, que lleva a aplicar la excepción al derecho a la información, puede darse en este sector por dos vías. A) Por un lado, puede encontrarse con que la propia realidad sanitaria genera situaciones susceptibles de ser objeto del límite al derecho. Determinadas acciones dirigiditas a proteger la salud de las personas pueden recogerse en la disposición legal que reconoce tal excepción. Puede ser el caso de la lucha contra una epidemia[1595]: la finalidad de evitar una epidemia para proteger la salud pública puede verse

[1594] STSJ Galicia 30 marzo de 2001, FJ 3: "Es por tanto una interpretación lógica (...) la que aconseja no una inteligencia estricta de los términos <<afectos a la defensa nacional>>, (...) sino, una acepción amplia de defensa de la nación que lleva a descartar luego el reducido sentido bélico y aceptar un sentido de protección social del Estado, si éste es un Estado –además de Derecho y Democrático- Social según el art. 1 de la CE, una de cuyas manifestaciones más importantes es la Seguridad Social (art. 41) de la que son beneficiarios los propios servidores de la Administración Local".

[1595] STC, 8 de junio de 1982, F.3: "(…) concepto de seguridad, la cual se centra en la actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadano, que son finalidades inseparables y mutuamente condicionadas. Afirmar esto no supone negar que una crisis sanitaria pueda amenazar la seguridad pública y justificar, en consecuencia, una intervención de las autoridades a las que corresponda

reconocida en los conceptos de seguridad pública o defensa nacional. Teniendo en cuenta el carácter tan amplio que se ha otorgado a estos términos, esta actividad puede considerarse recogida en los mismos. En estos casos la excepción a la obligación de informar podría ser aplicada.

B) Por otro, puede ocurrir que el tratamiento de los datos sanitarios con las finalidades recogidas en el artículo comentado se lleve a cabo fuera de la realidad sanitaria, en el ejercicio de acciones distintas a la protección de la salud. Esto sucede cuando los datos sanitarios son empleados con objetivos estrictamente policiales. En estos supuestos, en ocasiones el tratamiento de datos lo realizan los profesionales sanitarios por encargo o solicitud de las Fuerzas y Cuerpos de Seguridad o Jueces y Tribunales, para después transmitir las conclusiones a estos últimos[1596]. Sin embargo, otras veces la manipulación se reduce a una cesión de los datos contenidos en las historias clínicas a las Fuerzas y Cuerpos Seguridad con fines policiales. En estos casos, la información sobre esta cesión podría verse exceptuada en aplicación del precepto que se comenta.

II.4.4.C. Otras excepciones.

Además de las excepciones que se acaban de señalar, recogidas en la Ley estatal, pueden reconocerse otros supuestos de excepción al derecho a la información previstos tanto en textos legales de ámbito europeo como en trabajos doctrinales.

A) Por un lado, se ha tratado de trasladar desde el ámbito estrictamente médico la excepción a la obligación de informar por motivos terapéuticos al sector de la protección de datos. Tanto la normativa estatal[1597] como la del Consejo de Europa[1598], reguladora de la autonomía del paciente, reconocen la posibilidad de aplicar la excepción al derecho a ser informado sobre el estado de salud de cada uno por razones terapéuticas: no se deberá informar al paciente cuando el conocimiento de dicha información pueda perjudicar su salud[1599].

En estas normas, la aplicación de esta excepción está vinculada a la información sobre la salud o sobre las características de un tratamiento sanitario que ha de aplicarse a un paciente. Puede haber casos en que esta información perjudique al propio paciente. El conocimiento de

su custodia. Incluso es de recordar que crisis sanitarias tales como epidemias y situaciones de contaminación graves pueden motivar la declaración del Estado de Alarma".

[1596] ETEBARRIA GURIDI, *La Protección...,* cit., 1998; ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999; ETXEBERRIA GURIDI, *Los Análisis...,* cit., 2000.

[1597] Artículo 5.4 LBAP: "*El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave (...)".*

[1598] Artículo 10 Convenio de Oviedo, 4 de abril de 1997, para la protección de los Derechos Humanos y la Dignidad del Ser Humano respecto a las aplicaciones de la Biología y la Medicina: "*2. Toda persona tendrá derecho a conocer toda información obtenida respecto a su salud (...)*

3. De modo excepcional, la ley podrá establecer restricciones, en interés del paciente, con respecto al ejercicio de los derechos mencionados en el apartado 2".

[1599] CANTERO MARTÍNEZ, *La Autonomía*..., cit., 2005, p. 21; RODRÍGUEZ LÓPEZ, *La Autonomía...,* cit., 2004, pp. 98-105 y pp. 131-132; STS, 4 abril 2000, FJ. 3, señala que en algunas ocasiones la información excesiva puede ser también mala para la asistencia eficiente.

determinados datos sobre su enfermedad puede hacer que tenga una reacción adversa. Así, la excepción a dicha información pudiera estar justificada por motivos terapéuticos.

Ha habido quien ha pretendido la aplicación de la excepción por razones terapéuticas en el ámbito de la protección de datos[1600]. Incluso el Consejo de Europa ha previsto esta posibilidad en relación a los datos sanitarios[1601]. Se trataría de limitar el derecho a la información reconocido en la LOPD por motivos terapéuticos. No parece que esta excepción pueda tener un amplio recorrido en el ámbito de la protección de datos, ni siquiera tratándose de datos sanitarios. Atendiendo a su contenido, la información sobre las características de un determinado tratamiento al titular difícilmente podrá perjudicarle. El que un paciente conozca las finalidades de la manipulación de los datos que le conciernen, así como los derechos de acceso, cancelación o rectificación sobre los mismos, etc. no puede causarle daño alguno. Comprender la excepción al derecho a ser informado por razones terapéuticas como aplicable al ámbito de la protección de datos de carácter personal, no parece justificado.

B) Por otro lado, la normativa supranacional ha recogido supuestos de excepción que no se prevén en la Ley estatal. La Directiva europea[1602], en lo que interesa al ámbito sanitario, reconoce la posibilidad de exceptuar la obligación de informar al titular de los datos *"cuando tal limitación constituya una medida necesaria para la salvaguarda de: g) la protección del interesado o de los derechos y libertades de otras personas".*

La posibilidad de aplicar esta excepción en el sector sanitario interno plantea alguna interrogante. En primer lugar, hay que preguntarse si en el contenido de este precepto cabe incluir la salvaguarda de la salud de las personas. En principio, parece que dentro de la expresión que se emplea, "protección del interesado o de los derechos y libertades de otras personas", puede incorporarse sin dificultad la protección de la salud. Cuando se habla de la protección del interesado se está empleando un concepto amplio, en el que cabría incluir la protección de su salud física y mental. Lo mismo ocurre cuando se habla de los derechos y libertades de terceros. Si el ejercicio de la obligación de informar afecta negativamente a la realización de las funciones sanitarias cabe plantearse la posibilidad de limitar el derecho a ser informado.

En segundo lugar, en la perspectiva de las fuentes del derecho, cabe señalar que la aplicación directa de una disposición de una Directiva europea en el ámbito interno es posible siempre y cuando se cumplan una serie de requisitos; fundamentalmente que la norma sea precisa e incondicional[1603]. Es cierto que la posibilidad de aplicar directamente los preceptos de una Directiva depende de las características de los sujetos implicados en la relación en que se pretenden alegar esos preceptos. Así, depende de si se trata de una relación vertical, entre la Administración y un particular[1604]; si es horizontal, entre particulares[1605]; o triangular, donde se

[1600] SÁNCHEZ CARAZO, *La intimidad...*, cit., 2000, pp. 134-135.
[1601] Punto 116 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa.
[1602] Artículo 13 Directiva 95/46/CE.
[1603] STJUE 5 de marzo de 1998, Solred Sa v. Administración General del Estado, C-347/96, FJ 28. LASAGABASTER HERRARTE, *Fuentes del Derecho…*, cit., 2007, p. 265.
[1604] STJUE 26 de febrero de 1986, Marshall v. West Hampshire Area Health Authority, C-152/84, FFJJ 48-49, la eficacia directa tiene plena aplicación en estos casos.

ven implicados, normalmente, dos particulares y la Administración[1606]. Sin embargo, más allá de esta circunstancia se entiende que en el precepto concreto de la Directiva europea sobre protección de datos que ahora se comenta se dan las condiciones previas necesarias para poder alegar dicha eficacia directa. En este caso la norma es incondicional: se trata de un claro mandato. En cuanto a la precisión, es cierto que la expresión "protección del interesado o de los derechos y libertades de otras personas" es un tanto vaga y que admite diversos supuestos. En un estadio ideal, la norma estatal habría concretado la previsión europea. No obstante, no puede desecharse su aplicación en el ámbito interno alegando su indeterminación, máxime teniendo en cuenta la ambigüedad de los conceptos que emplea la Ley interna al fijar excepciones. De esta manera, en el ámbito interno podría aplicarse la excepción al derecho a la información que la Directiva europea reconoce. La protección del interesado y de los derechos y libertades de otras personas se erige en causa de excepción. La posibilidad de aplicar este límite en el ámbito sanitario ha de ser, no obstante, matizada. Podría desprenderse, partiendo de la letra de la norma europea, que cuando esté en juego la salud de una persona el derecho a ser informado queda automáticamente exceptuado. Si se aceptara este criterio sería prescindible la información general sobre las condiciones en las que se va a realizar el tratamiento de datos sanitarios, dirigida a todos los usuarios del sistema sanitario, a la que antes se ha hecho referencia. Dichos usuarios desconocerían los parámetros en los que se va a realizar la manipulación de sus datos.

Es evidente que esta situación sería inasumible desde el punto de vista del respeto al derecho a la autodeterminación informativa, puesto que el control sobre los datos de cada uno quedaría anulado. Como argumento dirigido a evitar que esta situación pueda aceptarse se encuentra el hecho de que la propia Directiva exige para aplicar dicha excepción que la misma "constituya una medida necesaria". No es aceptable que la protección de la salud del interesado o de un tercero conlleve, en todo caso, la excepción al derecho a ser informado. Dentro de los supuestos en que la salud de las personas está en juego, sólo podrá aplicarse la excepción cuando sea estrictamente necesario. Entra en juego, otra vez, el principio de proporcionalidad de tanta cita. En general, esta excepción que tiene como base la Directiva plantea la posibilidad de que, en determinadas circunstancias en que la salud de las personas está en juego, pueda limitarse el derecho a la información: situaciones de urgencia, por ejemplo. Necesariamente, la información general sobre las características fundamentales de todo tratamiento de los datos de salud dentro de un sistema sanitario no puede anularse basándose en esta excepción. Esta limitación constituiría una medida desproporcionada, innecesaria, no ajustada a Derecho. Más allá de esta información general, la información individualizada a la que se ha hecho referencia más arriba, concerniente a operaciones puntuales de las que nace un nuevo tratamiento, sí podría verse exceptuada basándose en el precepto que ahora se analiza. En todo caso, habría que analizar cada situación para concluir si la limitación del derecho es proporcional o no.

[1605] STJUE 14 de julio de 1994, Paola Faccini Dori v. Recreb Srl, FJ 20, señala que una Directiva no puede crear por sí misma obligaciones a cargo de particulares, por lo que resulta imposible la aplicabilidad directa de esta norma en estas relaciones.

[1606] STJUE 4 de enero de 2004, The Queen v. State for Transport, Local Government and the Regions, C-201/2002, FFJJ 56-58, por su parte, reconoce la posibilidad de aplicar las Directivas de forma directa en las relaciones triangulares, cuando de dicha aplicación directa no deriven de manera directa obligaciones a particulares. LASAGABASTER HERRARTE, *Fuentes del Derecho…*, cit., 2007, pp. 267-268.

C) Por último, la Recomendación del 97 relativa a la protección de datos médicos recoge también unos supuestos de excepción aplicables a los datos sanitarios. Lo cierto es que, en su mayor parte, en esta recomendación se reconocen para el ámbito sanitario las excepciones dispuestas en la Directiva y también en la LOPD[1607]. No obstante, en su articulado se concretan dos excepciones que tienen aplicación directa en el ámbito sanitario y que no aparecen en las otras normas.

Primero, dispone la recomendación que el derecho a ser informado se verá exceptuado cuando esté en juego la salud pública[1608]. Esta excepción no plantea grandes problemas pues parece de sentido común entender que la salud pública constituye un fin lo suficientemente digno para limitar el derecho a recibir información. La Ley estatal no la reconoce de manera expresa. Sin embargo, podría interpretarse que queda recogida dentro de alguno de los conceptos de seguridad pública o defensa nacional que emplea la LOPD, y que justifican la excepción del derecho a la información. Hay que tener en cuenta que la salud pública constituye en el ordenamiento estatal un bien jurídico de gran relevancia cuya salvaguarda, como ya se ha visto antes, merece de medidas extraordinarias entre las que se podría incluir la excepción al derecho a ser informado[1609]. En todo caso, y como se ha repetido en numerosas ocasiones, será necesario atender al principio de proporcionalidad para que la aplicación de la excepción sea ajustada a derecho.

En segundo lugar, se recoge en la recomendación otro extremo de relevancia. Se trata de una regulación dirigida específicamente al ámbito sanitario, y que en esencia resume perfectamente el espíritu que ha de inspirar toda excepción al derecho a ser informado: "*en emergencias médicas, los datos considerados necesarios para el tratamiento médico pueden recogerse previamente a la información"*[1610]*.*

De estas líneas se desprende la idea de que en situaciones en que la información al paciente sea especialmente complicada por su estado, o cuando esta información resulta un obstáculo en la realización de la tarea médica o asistencial, puede retrasarse en el tiempo hasta que dicha información sea posible. No se trata de una excepción propiamente dicha, sino de un retraso o prórroga a la hora de llevar a cabo la información. En este caso la prórroga no se establece, como lo hacía la Ley estatal, sólo para los supuestos en que los datos se recaban de fuentes diferentes al titular. Aquí, la posibilidad de retrasar la información se justifica debido a las características especiales del caso, que hace que la información inmediata sea imposible.

En esta disposición se reconoce la dificultad que en algunos casos se da para hacer efectivo el derecho a la información. Se refiere a los casos de emergencia, pero se podrían añadir situaciones que se viven en la práctica diaria: cesiones de datos entre órganos diferentes, tanto dentro como fuera del sistema sanitario con diferentes fines, situaciones generadas por la falta de tiempo para la asistencia, entre otras. Ante determinadas circunstancias se permite que el ejercicio de la información se prorrogue.

[1607] Artículo 5.6.a) R (97)5.
[1608] Artículo 5.6.a.ii) R (97)5.
[1609] LO 3/1986 14 de abril, de Medidas Especiales en materia de Salud Pública.
[1610] Artículo 5.6.b) R (97) 5.

La máxima que establece la Recomendación de que aunque sea más tarde se debe informar, ha de ser respetada. Si bien es cierto, como se indicara más arriba, que las recomendaciones del Consejo de Europa no configuran normas jurídicas directamente vinculantes para los estados, hay que recordar que constituyen un *soft law* de gran valor, sobre todo a la hora de interpretar la normativa interna.

En general, si bien las excepciones que se han analizado pueden tener cabida en el ámbito sanitario, hay que interpretar que como norma general se han de poner los medios necesarios para llevar a cabo el derecho a ser informado. Más allá de este criterio, la posibilidad de prorrogar el deber de informar abre la puerta para que esta obligación pueda ser ejercida con mayor flexibilidad, alternativa que ha de ser vista con buenos ojos en el ámbito sanitario.

II.5. Sobre la consideración como infracción leve de la falta de información en el tratamiento de datos.

La forma en que la Ley estatal sanciona la falta de información en el tratamiento de datos de carácter personal plantea una serie de dudas que han de ser, cuando menos, expuestas. La LOPD establece que la recogida de datos, que tiene como fuente al propio titular y que se lleva a cabo sin informar al afectado cuando dicha información es necesaria, constituirá una infracción leve. En cambio, cuando la falta de información se da en la recogida de datos que tiene como fuente no al propio afectado sino a una tercera persona o una fuente accesible al público, la infracción será calificada como grave. Esta distinción tiene sentido. Cuando los datos son recabados del propio titular éste tiene conocimiento de que algo va a ocurrir con los mismos. En la medida en que es él mismo el que transmite los datos al que será responsable del fichero, puede entenderse que el paciente conoce que la información que le concierne y que ha comunicado a otra persona va a ser manipulada de alguna manera. En cambio, cuando los datos son recabados no del propio titular de los datos sino de otra fuente, si no se lleva a cabo la información el titular no tendrá conocimiento alguno de que algo está sucediendo con sus datos, con lo que el derecho a la autodeterminación informativa queda completamente anulado.

Sin embargo, y si bien esta clasificación puede tener sentido, lo cierto es que se plantean algunas dudas sobre la consideración como infracción leve o grave de la ausencia de información en un tratamiento de datos.

Atendiendo a la Ley se observa que la manipulación de datos relativos a la salud de las personas sin el consentimiento de su titular, cuando dicho consentimiento es necesario, constituye una infracción muy grave[1611]. Por lo tanto, la ausencia del consentimiento constituye una infracción muy grave mientras que la falta de información necesaria supone simplemente una infracción leve o grave dependiendo del caso. No deja de ser cuando menos llamativa esta distinción, pues no hay que olvidar que la información es requisito indispensable para que un consentimiento sea válido.

[1611] Artículo 44.4.c) LOPD: "*Son infracciones muy graves: c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7*".

Antes se ha dicho que el consentimiento sin información no es consentimiento pues supone aprobar algo que no se conoce. Siendo esto así, no parece que sea coherente desde el punto de vista jurídico que estas dos infracciones sean calificadas de manera diferente cuando las consecuencias que acarrean son idénticas. Si la falta de información conlleva que el consentimiento que se vaya a dar no sea válido, ¿cómo es posible que la falta de consentimiento en el tratamiento de datos de salud constituya una infracción muy grave y la falta de información una infracción leve o grave?

Partiendo de esta consideración se podría llevar a cabo la siguiente interpretación de la regulación del sistema sancionador de la LOPD en este punto. Cuando el consentimiento expreso es requisito indispensable para el tratamiento de los datos de salud, su manipulación sin la información pertinente constituye una infracción muy grave en la medida en que dicha falta de información conlleva también la invalidación del consentimiento que se haya podido dar.

Por otro lado, la crítica a la consideración del incumplimiento del deber de informar como infracción leve o grave encuentra apoyo en otro argumento. Cuando el consentimiento resulta exceptuado para el tratamiento de los datos de salud pero el derecho a la información permanece vigente, esta información se convierte en la única forma de que el titular controle los datos que le conciernen. Efectivamente, si no se le da esa información, no tiene forma de ejercer el derecho a la autodeterminación informativa. Desde este punto de vista tampoco se comprende que esta falta, que afecta de manera tan negativa a este derecho fundamental, sea considerada simplemente como leve o grave.

Hay que tener en cuenta, en este sentido, que la Ley considera que la recogida de datos en forma engañosa y fraudulenta constituye una infracción muy grave. Fácilmente se podría calificar en algunos casos una recogida de datos sin la debida información, aprovechándose el responsable del fichero, por ejemplo, del desconocimiento del titular de los datos, como una recogida engañosa y fraudulenta. Más arriba se hacía referencia a que el respeto a la obligación de informar deriva también de la buena fe. Así, podría interpretarse que dejar de informar al titular de unos datos de manera voluntaria aprovechándose de una situación determinada constituye una actuación engañosa y fraudulenta calificable como infracción muy grave.

III. EL DERECHO A OTORGAR EL CONSENTIMIENTO.

III.1. Introducción.

Se ha comentado que el consentimiento informado constituye el principal exponente de la autodeterminación de las personas respecto a sus datos[1612]. La capacidad de controlar la información sobre uno mismo se manifiesta sobre todo en la facultad de autorizar o no los tratamientos que se vayan a dar a la misma[1613]. Precisamente por ello la práctica totalidad de la

[1612] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 219; GAY FUENTES, *Intimidad y Tratamiento...,* cit., 1995, p. 77; CARDONA RUBERT, *Informática y Contrato...,* cit., 1999, pp. 116-117; GOÑI SEIN, *La Videovigilancia...,* cit., 2007, pp. 178-179.

[1613] STSJ de Madrid, 15 de enero de 2004, FJ 6º, haciéndose eco de lo fijado por el TS: los "poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos

doctrina, y también la jurisprudencia, ha considerado esta figura como la institución más relevante en la protección de los datos de carácter personal[1614].

Como se ha dicho al iniciar este capítulo, hay que tener en cuenta que el derecho a la autodeterminación informativa se fundamenta en el principio de autonomía del individuo[1615], es decir, en la consideración de la persona como sujeto maduro capaz de decidir sobre las cosas que le afectan, en este caso sobre las informaciones concernientes a sí misma[1616]. Este principio de autonomía deriva a su vez de otros tan consagrados en la norma suprema como el de libertad, el libre desarrollo de la personalidad o la dignidad[1617]. Pues bien, expresión principal de esta autonomía y de esa madurez es el consentimiento[1618]. No hay mayor autodeterminación con respecto a los datos de cada uno que la capacidad de decidir qué hacer con ellos[1619]. Como punto de partida, por lo tanto, se puede entender que cada persona es propietaria de sus datos y éstos sólo podrán manipularse cuando su titular así lo permita[1620].

En el ámbito sanitario la cuestión principal a aclarar en relación al consentimiento será si éste es necesario o no para la recogida y posterior tratamiento de los datos sanitarios. Habrá que partir de la idea de que tanto la recogida como el tratamiento de este tipo de información requieren de la autorización del titular para poder llevarse a cabo. Toda excepción a esta exigencia deberá estar justificada. Como se verá en las líneas que siguen, los límites a la facultad de consentir este tipo de operaciones en el ámbito sanitario son múltiples. No obstante, es interesante analizar la figura del consentimiento para comprender mejor el régimen que sigue la protección de datos en este ámbito.

personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular".

[1614] APDCM, *Guía de Protección...*, cit., 2004, p. 287; HERRÁN ORTIZ, *La Violación...*, cit., 1998, p. 254; MURILLO DE LA CUEVA, *Informática y Protección...*, cit., 1993, p. 61; ARENAS RAMIRO, *El Derecho...,*cit., 2006, p. 102; FERNÁNDEZ LÓPEZ, "Principio de Consentimiento…", cit., 2010, p. 454. SSAN, 19 de octubre de 2005, FJ 2 y 1 de junio de 2005, FJ 6.

[1615] Informe Belmont, 30 septiembre 1978, que sienta los Principios de Bioética respecto a la Autonomía de las Personas, Beneficencia y Justicia, y fija los Requisitos Básicos del Consentimiento Informado, la Valoración de Riesgos y Beneficios y la Selección de los Sujetos: "una persona autónoma es un individuo que tiene la capacidad de deliberar sobre sus fines personales, y de obrar bajo la dirección de esta deliberación. Respetar la autonomía significa dar valor a las consideraciones y opciones de las personas autónomas, y abstenerse a la vez de poner obstáculos a sus acciones a no ser que éstas sean claramente perjudiciales para los demás".

[1616] DENNINGER, "El Derecho...", cit., 1997, p. 272: "La Ley Fundamental y sus intérpretes parten de que el hombre es una <<personalidad capaz de organizar su vida con responsabilidad propia>>. Esta organización de la vida sólo puede tener éxito si el individuo al mismo tiempo que puede mandar sobre su propia conducta (...) también tiene influencias sobre lo que los demás esperan de él y como se comportan hacia su persona. Dicho de otra forma: el individuo tiene que tener la posibilidad de influir sobre su ambiente social, decidiendo él mismo dónde, cuándo, cómo y en qué contexto quiere presentarse a su ambiente"; GOÑI SEIN, *La Videovigilancia...,* cit., 2007, p. 95.

[1617] DÍAZ PINTOS, "El Consentimiento...", cit., 1998, p. 25; REQUERO IBÁÑEZ, "El Consentimiento...", cit., 2002, pp. 892-894; BROGGI TRIAS, "Algunos Problemas...", cit., 1997, p. 211.

[1618] SÁNCHEZ CARO, "Consentimiento Informado...", cit., 2004, p. 163.

[1619] FERNÁNDEZ SALMERÓN, *La Protección de los dato…,* cit., 2003, p. 91.

[1620] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 32; GUICHOT, *Datos Personales...,* cit., 2005, p. 234.

III.2. Definición.

Para determinar el contenido del consentimiento es necesario atender primero a las definiciones que las diferentes normas han dado de dicho concepto, pues del análisis de estas regulaciones se podrán deducir los requisitos que ha de cumplir para que sea válido.

La LOPD y las normas de las diferentes Comunidades Autónomas que han regulado la protección de datos[1621], partiendo de lo que la Directiva europea dispone sobre esta cuestión[1622], definen el consentimiento como *"toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen".* La antigua Ley estatal no recogía definición alguna del consentimiento. Esta situación generaba cierta inseguridad, pues se hacía más difícil determinar cuáles tenían que ser los requisitos que la autorización debía cumplir para ser válida. De esta manera, hay que entender en principio como positiva la inclusión de esta definición en la nueva norma.

Como ha señalado la jurisprudencia, la actual Ley acude a un criterio sustantivo para definir este derecho[1623]. En este sentido, es subrayable la inclusión en la definición de la Ley del adjetivo "inequívoco". Esta exigencia en un inicio sugiere una regulación garantista del derecho a la autodeterminación informativa[1624]. No obstante, como se verá, el empleo de este calificativo plantea problemas de interpretación a la hora de determinar la forma que deberá adoptar dicho consentimiento.

La LBAP, por su parte, también da una definición del consentimiento. Sin embargo, en este caso este derecho se vincula con la autonomía del paciente respecto a su salud, no a sus datos de carácter personal. Se entiende por consentimiento informado "*la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud"*. En las diferentes normas reguladoras de los diversos aspectos que componen la realidad sanitaria es común que se recoja una definición sobre el derecho a otorgar el consentimiento, aunque todas emplean, prácticamente, idénticos términos[1625].

Se puede apreciar, tanto en el ámbito de la protección de datos como en el de la autonomía del paciente, que la definición del consentimiento responde al mismo esquema y recoge los mismos elementos, con pocas variaciones. Las definiciones dadas por la jurisprudencia, como se ha visto al analizar el concepto más genérico de "consentimiento informado", son también similares.

[1621] Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, artículo 3.h), y Ley 2/2004, de 25 de febrero, de Ficheros de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos, artículo 3.g).

[1622] Artículo 2.h) Directiva 95/46/CE: "*Consentimiento del interesado: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan*".

[1623] SAN 18 de julio 2007, FJ 4.

[1624] SAN 16 de octubre 2003, FJ 3.

[1625] Artículo 3.f) Ley 14/2007, 3 de julio, de Investigación Biomédica: "*Consentimiento: manifestación de la voluntad libre y consciente válidamente emitida por una persona capaz, o por su representante autorizado, precedida de la información adecuada*".

La valoración de estas definiciones, especialmente de la incluida en la norma reguladora de la protección de datos, ha de venir de la mano de un análisis de cada uno de los elementos que las componen. Al realizar este ejercicio será necesario acudir, en algún caso, a lo que dispone el CC en relación a los requisitos necesarios para la celebración de los contratos[1626].

III.3. Contenido.

Partiendo de lo dispuesto en las normas indicadas se pueden apuntar los siguientes como requisitos necesarios para que el consentimiento sea válido: habrá de ser libre o voluntario, inequívoco, específico, consciente, e informado.

III.3.1. Sobre el carácter libre del consentimiento.

III.3.1.A. Especial referencia a la posibilidad de revocar el consentimiento.

En primer lugar, el consentimiento del titular de los datos tiene que ser libre o voluntario. Por libre se entiende que no puede estar sometido a ningún tipo de coacción o intimidación que lleve a alterar el sentido de la voluntad de dicha persona[1627].

Es interesante, en este sentido, exponer brevemente lo que dispone el CC al respecto[1628]. Se considera en esta norma que cuando se emplea una fuerza irresistible para obtener la autorización, en este caso del titular de los datos, se estará ante un supuesto de violencia que invalida dicho consentimiento. En la misma línea, cuando al afectado se le inspira el miedo "racional y fundado" de que su persona o sus bienes, o las personas o bienes de su cónyuge, descendientes o ascendentes van a sufrir algún daño grave e inminente se entenderá que hay intimidación. A la hora de valorar si existe o no intimidación habrá de estarse a la edad y condición del afectado.

Los tribunales se han referido a la figura de la intimidación exigiendo una serie de requisitos para que la misma cause el efecto de invalidar el consentimiento: que la coacción o la fuerza que se ejerza sobre la persona que ha de otorgar la autorización se valga de un acto injusto, y no "del ejercicio correcto y no abusivo de un derecho"; que la intimidación constituya una amenaza injusta o ilícita bastante para determinar la voluntad del sujeto, lo que requiere que se amenace con un mal inminente y grave y tan fuerte y creíble que obligue a quien la padece a que su voluntad se determine en sentido contrario a sus intereses[1629]; que debido al miedo del daño o perjuicio que puede sufrir, lleve a este último a otorgar un consentimiento que no se quiere emitir. Deberá consistir en una amenaza fundada y racional, y no un temor leve, de que se puede llegar a sufrir un mal de entidad[1630].

[1626] Artículos 1.261 y siguientes CC.
[1627] ARENAS RAMIRO, "El Principio del Consentimiento…", cit., 2007, p. 170.
[1628] Artículo 1.267 CC, modificado por la Ley 11/1990, 15 de octubre, sobre reforma del Código Civil en aplicación del Principio de No Discriminación por Razón de Sexos.
[1629] AP de Sevilla 20 de junio de 2006, FJ 2; AP de Valencia 10 de abril de 2006, FJ 2; AP de Vizcaya 30 de noviembre de 2004, FJ 4.
[1630] STSJ de Madrid 26 de noviembre de 2002, FJ 2: "para que concurra intimidación debe darse, un doble requisito: Una actitud o comportamiento tendente a inspirar: a) el temor de sufrir un daño, distinto al legítimo ejercicio de un

Es obvio que lo dispuesto en el CC y en la jurisprudencia es aplicable al consentimiento en la protección de datos. No obstante, en este ámbito los problemas jurídicos que ha planteado el requisito de la libertad no se vinculan tanto a la posibilidad de que la autorización se haya podido recabar de una forma violenta, sino a saber si la libertad para otorgar el consentimiento conlleva, a su vez, la libertad de revocarlo y, en caso de que sea posible, cómo podrá llevarse a cabo dicha revocación.

La libertad de otorgar el consentimiento supone también la libertad de revocarlo[1631]. Ha de entenderse por revocación la acción del titular de los datos de dejar sin validez o efecto el consentimiento prestado previamente[1632]. La LOPD recoge expresamente esta posibilidad. Sin embargo, según la Ley, la revocación podrá darse siempre y cuando exista causa justificada para ello y no se apliquen efectos retroactivos a la misma[1633]. El RDLOPD reconoce igualmente esta facultad, concretando además que el responsable no podrá fijar sistemas complejos para llevar a cabo la revocación que dificulten su ejercicio[1634].

La previsión de la revocación por la Ley está plenamente justificada. Si realmente se considera que el consentimiento ha de ser libre, parece razonable comprender que esta libertad conlleva también la posibilidad de desautorizar lo autorizado. El propio Consejo de Europa, precisamente al regular la protección de datos sanitarios, entiende que el consentimiento será libre cuando el titular de los datos tenga la facultad de rechazarlo, retirarlo o modificar los términos y condiciones en que se dio[1635]. Por el contrario, no se puede asumir aquí la exigencia

---

derecho que pudiere perjudicar a la contraparte. b) Que las circunstancias de edad y condiciones personales del sujeto permitan afirmar que este temor es racional y fundado, y a la vez, suficientemente grave como para doblegar su voluntad".

[1631] RIPOL CARULLA, "La Protección... (Parte II)", cit., 1997, p. 116.

[1632] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit. 2003, p. 252: "Tradicionalmente, se define la revocación como el negocio jurídico unilateral y recepticio mediante el cual se deja sin efecto la declaración de voluntad emitida anteriormente en aquellos casos en que así lo permita la ley."

[1633] Artículo 6.3, LOPD: *"El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos"*,

[1634] Artículo 17 RDLOPD: "*1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.*

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre".

[1635] Punto 131 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: *"Consent is" free" if the data subject has the possibility to refuse his/her consent, to withdraw it or to modify the terms and conditions of consent"*.

que plantea la LOPD de que, para que la revocación sea válida, el titular de los datos tenga que argumentar y demostrar una "causa justificada" dirigida a motivar la revocación[1636]. Aunque algún autor parece haber considerado adecuado el requisito que se plantea[1637], no se comparte aquí dicha interpretación. Desde un inicio esta cuestión ha sido una de las más debatidas.

Como se acaba de afirmar, si el consentimiento es un acto de control por parte del titular sobre sus propios datos, que lo da en plena libertad, esta misma libertad tiene que ser la que aliente la revocación del mismo consentimiento[1638]. La exigencia de la causa justificada supone una limitación de esa autonomía que no tiene fundamento alguno, más aún si se tiene en cuenta que la revocación no tiene efecto retroactivo[1639].

Esta línea interpretativa se puede deducir del propio ordenamiento. La LOPD, al regular la cesión de datos reconoce la posibilidad de revocar el consentimiento y, en este caso, no exige causa justificativa alguna para llevar a cabo dicho ejercicio. Incluso el nuevo reglamento que desarrolla la Ley, consciente de que la revocación ha de constituir una operación que quede a voluntad del titular de los datos, flexibiliza lo dispuesto por la LOPD señalando que el responsable del fichero deberá establecer o fijar un sistema sencillo para llevar a cabo dicha operación[1640].

En otros ámbitos del Derecho la revocación del consentimiento tampoco exige causa justificativa. En el campo del derecho de la información, el consentimiento puede legitimar una intromisión en los derechos fundamentales al honor, intimidad y propia imagen[1641]. No obstante, esta autorización puede ser revocada en cualquier momento, con la única condición de que se indemnicen los daños y perjuicios que se hayan podido causar debido a dicha revocación[1642]. En el caso del derecho a consentir un tratamiento sanitario o médico determinado para hacer frente a una enfermedad, la LBAP tampoco exige que haya causa alguna que justifique la revocación de la autorización[1643].

[1636] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 120; ZABÍA DE LA MATA, *"*Tratamiento de datos…*",* cit., 2008, p. 207; SEOANE RODRÍGUEZ, "De la Intimidad... (Parte II)", cit., 2002, p. 159.
[1637] GAY FUENTES, *Intimidad y Tratamiento...,* cit., 1995, p. 77.
[1638] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, p. 256; GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 260.
[1639] CONDE ORTIZ, *La Protección...,* cit., 2005, p. 96; FERNÁNDEZ LÓPEZ, "Principio de consentimiento…", cit., 2010, p. 470.
[1640] ZABÍA DE LA MATA, *"*Revocación…*",* cit., 2008, pp. 206-208.
[1641] Artículo 2.2 LO 1/1982, de 5 de mayo de 1982, de Protección Civil de los Derechos al Honor, Intimidad Personal y Familiar y a la Propia Imagen: "*No se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso*".
[1642] Artículo 2.3 LO 1/1982, 5 de mayo de 1982, de Protección Civil de los Derechos al Honor, Intimidad Personal y Familiar y a la Propia Imagen: "*El consentimiento a que se refiere el párrafo anterior será revocable en cualquier momento, pero habrán de indemnizarse, en su caso, los daños y perjuicios causados, incluyendo en ellos las expectativas justificadas*"; STC 25 de abril de 1994.
[1643] Artículo 8.5 LBAP: "*El paciente puede revocar libremente por escrito su consentimiento en cualquier momento*". BLAS ORBÁN, *El equilibrio...*, cit., 2006, p. 148.

En definitiva, debería bastar la mera manifestación de voluntad del titular de los datos para que se dé la revocación del consentimiento. Exigir más requisitos que el que se acaba de citar supone limitar la capacidad de éste de manera injustificada.

A mayor abundamiento, la exigencia de una causa justificativa para la revocación plantea otro problema de envergadura. En la práctica, aplicando el contenido de la Ley, sería el responsable del fichero quien interpretaría si existe o no causa suficiente para llevar a cabo la revocación. Si considerara que tal causa no existe el consentimiento permanecería vigente y el tratamiento de datos podría continuar. En este caso sería este responsable el que decidiría si puede o no manipular la información de otra persona, sin mayor control que el que se pudiera llevar a cabo *a posteriori* por parte de la agencia de protección de datos correspondiente y, en su caso, por Jueces y Tribunales, sobre si hubo o no causa justificativa para revocar el consentimiento. Se abriría la puerta a que el responsable pudiera actuar de manera discrecional, cuando no arbitraria, fundamentándose en una supuesta falta de justificación[1644]. Ayudaría, además, a que tuviera un ámbito de actuación especialmente amplio el empleo por parte de la Ley de un concepto tan vago como el de "causa justificada", sin determinar un criterio que defina qué motivos pueden llevar a entender que existe dicha causa.

Lógicamente, la posibilidad de que el centro de control de unos datos de carácter personal se traslade desde su titular hasta el responsable que los manipula ha de ser rechazada. Por eso, la jurisprudencia ha comprendido acertadamente que el concepto de "causa justificada" ha de entenderse en sentido amplio y favorable al titular de los datos[1645]. Es decir, no pueden limitarse las causas justificativas de la revocación a contados supuestos de difícil realización sino que ha de interpretarse que la más leve causa puede acarrear la revocación del consentimiento.

Siguiendo la línea interpretativa que marca la jurisprudencia que se acaba de citar se puede concluir que, a pesar de que la letra de la Ley exija una causa justificativa para que el consentimiento otorgado por el titular de los datos quede invalidado, en la práctica, el principio de libertad de cada individuo a controlar la información que le concierne ha de llevar a que este requisito se interprete de manera laxa.

III.3.1.B. La libertad a la hora de dar el consentimiento en el ámbito sanitario.

En el ámbito sanitario el requisito de la libertad a la hora de otorgar el consentimiento no plantea mayores problemas. La autorización en la recogida y tratamiento de datos sanitarios con la finalidad de salvaguardar la salud de las personas se deberá dar con total libertad. No se concibe que pueda llevarse a cabo una recogida de datos a partir de un consentimiento viciado por el empleo de la fuerza o por cualquier otra causa. Otra cosa serán las excepciones que puedan imponerse a este consentimiento para la recogida y tratamiento de datos de salud en el ámbito sanitario, lo que más adelante se verá.

[1644] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 48.
[1645] SAN 17 abril 2007, FJ 3.

Esta misma libertad debe justificar en este ámbito la posibilidad de revocar el consentimiento inicialmente dado[1646]. Lo mismo que tiene autonomía para transmitir o no sus datos a la Administración sanitaria para que ésta pueda manipularlos posteriormente con la finalidad de proteger su salud, el titular tendrá también la facultad de desautorizar lo autorizado. Se han planteado como argumentos para justificar la revocación el que, por ejemplo, una investigación se lleve a cabo por un equipo distinto al inicial o que la entidad médica responsable de los ficheros cambie de responsable por una fusión[1647]. Puede suceder también que el usuario, con la finalidad de salvaguardar su intimidad, solicite la revocación y posterior cancelación de determinada información que se refiere a su persona. Sin embargo, se entiende aquí que más allá de estos supuestos concretos la propia voluntad del titular ha de bastar para revocar el consentimiento dado para la recogida de datos para su posterior tratamiento con fines sanitarios. En el campo sanitario las normas reconocen en diferentes supuestos la capacidad de los pacientes de revocar el consentimiento dado a un tratamiento médico determinado[1648]. Si en estos casos la autonomía de los usuarios lleva a aceptar esta facultad, sin necesidad de demostrar un interés específico, no parece descabellado reconocer que la misma facultad se debe atribuir a las personas con respecto a sus datos de carácter personal. Esta facultad se debe imponer siempre que no haya un bien jurídico suficiente que justifique limitar esta capacidad de revocar.

En el ámbito sanitario la limitación de la facultad de revocar la autorización viene no tanto por la necesidad de encontrar una causa justificativa, sino por otros motivos. Hay que tener en cuenta que la revocación del consentimiento impediría que los profesionales sanitarios manipularan los datos, lo que dificultaría la realización de su tarea protegiendo la salud de las personas. La posibilidad de que la revocación ponga en riesgo la salud, bien sea la del propio titular de los datos o de terceras personas, hace que en el ámbito sanitario esta figura tenga poco recorrido. En realidad, la limitada aplicabilidad de la revocación en este sector deriva porque, adelantando argumentos que se darán posteriormente, también el derecho a otorgar el consentimiento encuentra su aplicabilidad reducida en este ámbito. Más adelante se verán cuáles son los límites que se pueden imponer a la autonomía del paciente en la recogida y tratamiento de datos. Estas excepciones motivarán también, como es lógico, la limitación de la capacidad de revocar el consentimiento. Si no hay consentimiento que emitir difícilmente podrá éste ser revocado.

I

[1646] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.
[1647] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 89.
[1648] Artículo 8.5 LBAP: "*El paciente puede revocar libremente por escrito su consentimiento por representación*". En el ámbito autonómico también pueden encontrarse referencias expresas a la posibilidad de revocación: artículo 5 Ley 11/2007, 26 de noviembre, reguladora del Consejo Genético, de Protección de Derechos de las Personas que se sometan a Análisis Genéticos y de los Bancos de ADN humano en Andalucía: "*1. La realización de análisis genéticos, ya sea con fines de asistencia sanitaria, pruebas de cribado genético o con fines de investigación biomédica, requiere el consentimiento informado, que se otorgará en un documento escrito, por la persona titular de la muestra biológica, tras haber recibido la información prevista en los artículos 12, 16.4 y 25 de esta Ley. En los supuestos previstos en la presente Ley, el consentimiento podrá prestarse por representación, en los términos expresados en el artículo 6.*
2. La persona otorgante del consentimiento informado podrá proceder libremente a su revocación en cualquier momento, con los efectos previstos en el artículo 24 de esta Ley, en su caso".

II.3.2. Sobre el carácter inequívoco del consentimiento.

III.3.2.A. El consentimiento oral y tácito como fórmulas permitidas por la normativa de protección de datos.

Como segundo requisito las normas exigen que el consentimiento sea "inequívoco". Así lo hacen tanto la LOPD como la Directiva europea[1649]. Se ha entendido por inequívoco lo "que no admite duda o equivocación"[1650]. La jurisprudencia ha señalado en algún caso que el consentimiento será inequívoco cuando sea incuestionable[1651]. Se cumplirá con este requisito, por lo tanto, cuando no haya lugar a dudas de que la voluntad del titular de los datos es la de autorizar su tratamiento[1652]. Cualquiera que sea la forma en que se dé la autorización ésta deberá aparecer como evidente[1653]. No obstante, ¿cómo se ha de interpretar esta consideración? Los problemas en este punto surgen a la hora de dar un contenido determinado a este término[1654], pues son diferentes las formas que puede adoptar el consentimiento, a saber: oral, escrito, expreso, tácito, presunto.

Ha habido quien ha equiparado el consentimiento inequívoco con el expreso e incluso con el escrito[1655], entendiendo que ésta es la única forma de que quede constancia segura de la existencia de la voluntad del titular de los datos. Como se verá, no parece que esté en el deseo del legislador exigir que la autorización del titular sea en todo caso expresa y escrita. La exigencia de que el consentimiento sea inequívoco se refiere a la forma de expresarlo, no a la necesidad de que quede constancia del mismo.

A) En primer lugar, se puede afirmar que el requerimiento de que el consentimiento sea inequívoco no exige, siempre, el carácter escrito del mismo, pues la autorización oral puede también no conllevar duda alguna sobre la voluntad del titular de los datos. Las normas dan pie a reconocer la validez de la forma oral. La LOPD, en la anteriormente criticada clasificación que realiza entre datos, se podría decir, comunes, sensibles e hipersensibles, exige para el tratamiento de los que revelen la ideología, afiliación sindical, religión y creencias, el consentimiento expreso y escrito[1656]. Para el resto de los datos, para los que no se exige expresamente el consentimiento escrito y entre los que se incluyen los sanitarios, habrá que interpretar que basta con que éste sea oral. En esta línea, el Consejo de Europa entiende con respecto al tratamiento de los datos sanitarios, que el consentimiento no tiene por qué ser escrito,

[1649] Artículo 7.a) Directiva 95/46/CE.
[1650] En http://www.rae.es/
[1651] SAN 9 mayo 2007, FJ 4.
[1652] SAN 15 de septiembre de 2001, FJ 3; LEGALIA, *La Protección...*, cit., 2002, p. 98.
[1653] SAN 18 de julio 2007, FJ 4.
[1654] DEL PESO NAVARRO, *Ley de Protección...,* cit., 2000, pp. 155-156.
[1655] RUIZ CARRILLO, *La Protección...*, cit., 2001, p. 44, se pregunta "qué diferencia existe entre otorgar un consentimiento inequívoco o prestarlo por escrito. El consentimiento otorgado por escrito siempre será inequívoco, pero el tácito, siempre podrá ser alegado, como equívoco, pues, en modo alguno puede demostrarse la declaración de voluntad manifestada expresamente sobre el extremo que se analiza; sólo presuponerse. Si se supone o presupone, ya no hay evidencia y si no la hay, el consentimiento ha de ser forzosamente equívoco".
[1656] Artículo 7.2 LOPD.

sino que perfectamente puede darse vía oral[1657]. El problema en el supuesto del consentimiento oral será probar su existencia[1658]. En varios casos la AEPD ha puesto de manifiesto el hecho de que es necesario recabar la autorización del titular de forma que quede constancia de ello[1659]. Evidentemente, la forma oral plantea problemas a este respecto, pero no por ello ha de rechazarse, pues como ha apuntado la jurisprudencia, la prueba puede llevarse a cabo partiendo de indicios[1660]. En todo caso, señala el RDLOPD, será el responsable del fichero quien deberá probar la existencia del consentimiento[1661].

B) Las principales dudas no se plantean en torno al carácter escrito u oral del consentimiento sino en torno a la posibilidad de que sea expreso, tácito o presunto, es decir, en relación a la forma de expresarlo. En segundo lugar, por lo tanto, hay que analizar si, en la medida en que tiene que ser inequívoco, toda forma de expresar el consentimiento será válida. Parece evidente que no.

Según la Real Academia lo expreso hace referencia a lo "claro, patente especificado"[1662], lo tácito a lo "callado, silencioso", a lo "que no se entiende, percibe, oye, o dice formalmente, sino que se supone e infiere"[1663], y lo presunto a lo "supuesto"[1664]. Estas mismas definiciones ha hecho suyas la AEPD en alguna de sus resoluciones[1665].

En algún caso, parte de la doctrina[1666] y alguna resolución judicial[1667] han aceptado el consentimiento presunto como válido. Se entiende aquí que esta fórmula no es aceptable en el

[1657] Punto 130 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: *"Free, express and informed consent given in writing is a requirement laid down in the recommendations on data protection in other sectors; for the processing of medical data, such consent need not be written; it can also be given orally, or by means of a recording, provided that the desired purpose of authenticating the data subject´s agreement is achieved"*.

[1658] TÉLLEZ AGUILERA, *Nuevas tecnologías…,* cit., 2001, p. 150; APDCM, *Guía de...,* cit., 2004, p. 289: "Debe recomendarse que siempre que se traten datos especialmente protegidos, con independencia de cuáles sean, se procure obtener constancia del consentimiento expreso en forma escrita, puesto que recae sobre el responsable del tratamiento la carga de la prueba de demostrar que se disponía del consentimiento, con ese especial atributo de expreso".

[1659] RUBÍ NAVARRETE, "Experiencias y...", cit., 2006, p. 260: en relación a la posibilidad de que para el tratamiento de datos de salud se requiera consentimiento escrito además de expreso: "En la mayor parte de las resoluciones de la AEPD en que el consentimiento de los datos de salud no consta expresamente por escrito, se ha declarado una infracción de dicha norma. Sin embargo, de ello no puede desprenderse la conclusión de que el consentimiento exigible debe ser siempre escrito, sino sólo que, en los casos analizados, no resultaba acreditada la prestación de un sentimiento expreso. De forma (p. 261) que ha sido una cuestión relacionada con la prueba del consentimiento y no con los requisitos exigibles legalmente el que ha determinado la declaración de las infracciones tipificadas en la LOPD".

[1660] SAN 1 de febrero de 2006, FFJJ 3 y 4; LESMES SERRANO, "Definiciones…", cit., 2008, p. 119.

[1661] Artículo 12.3 RDLOPD. PUENTE ESCOBAR, "Consentimiento del afectado…", cit., 2009, p. 40.

[1662] FERNÁNDEZ LÓPEZ, "El Consentimiento...", Cit., 2003, el consentimiento expreso es el que "se dirige de modo directo e inmediato a dar a conocer la voluntad interna del declarante".

[1663] FERNÁNDEZ LÓPEZ, "El Consentimiento...", Cit., 2003, entiende que en el consentimiento tácito "el sujeto no manifiesta de modo directo su voluntad sino que realiza una determinada conducta que por presuponer necesariamente tal voluntad, es valorada como declaración por el ordenamiento jurídico".

[1664] Memoria AEPD, 1994: el "consentimiento expreso se manifiesta mediante un acto positivo y declarativo de la voluntad. El consentimiento tácito se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume o se presupone como un acto de aquiescencia o aceptación. Por último, cabe el consentimiento presunto, que no se deduce ni de una declaración, ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación".

[1665] Resolución de archivo de actuaciones de la AEPD, expediente nº E/00272/2008, 19 de junio de 2009.

[1666] SANZ CALVO, "*Consentimiento…*", cit., 2008, p. 194.

[1667] SAN 20 septiembre de 2006, FJ 6.

ordenamiento. El consentimiento presunto parte simplemente de la suposición del responsable del fichero de haber recabado la autorización del titular de los datos, suposición que se desprende del comportamiento del afectado[1668]. De este modo sería el responsable del fichero el que determinaría, deduciéndolo del comportamiento del titular de los datos, si ha habido consentimiento o no. Así se trasladaría al responsable del tratamiento la capacidad de decidir sobre la posibilidad o no de tratar la información sobre una determinada persona. Partiendo de esta afirmación no se puede considerar el consentimiento presunto como inequívoco[1669], pues, como el propio nombre indica, tiene como base una suposición o deducción que de ninguna manera cumple con la exigencia de que no haya duda sobre la emisión de la autorización. Como se afirma en alguna resolución de la AEPD, atendiendo a lo establecido en la jurisprudencia, lo inequívoco no admite deducciones de meros actos realizados por el afectado, sino que exige que exista expresamente una acción u omisión que refleje la existencia del consentimiento[1670]. La aceptación de una figura como el consentimiento presunto atentaría, se entiende aquí, contra la esencia misma del derecho a la autodeterminación informativa, pues menoscabaría la capacidad de control del titular de los datos al permitir que sea el responsable del fichero quien decida si existe o no el consentimiento[1671].

En cuanto al consentimiento tácito, prácticamente toda la doctrina ha admitido, a efectos de la aplicación de la LOPD, que el mismo deriva del silencio del titular[1672]. En algún caso se ha identificado esta forma de autorizar un tratamiento como una variante del consentimiento presunto, en un sentido más amplio que el que se le otorga en este trabajo[1673]. Esta última idea podría llevar a la negación de la validez de la autorización tácita[1674]. No obstante, estas dos formas de otorgar el consentimiento no tienen las mismas características y el tácito, entendido en un sentido más restrictivo, puede tener cabida en el ordenamiento. Se interpreta aquí, al contrario de lo que señalan otros autores, que el consentimiento tácito se identifica con la autorización derivada del silencio del titular de los datos.

En un principio, y si se parte de las definiciones dadas por la Directiva y la LOPD del concepto "consentimiento", parece desechable la autorización tácita como fórmula para habilitar el tratamiento de datos. Dichas definiciones toman como punto de partida la expresión "declaración de voluntad", lo cual sugiere que ha de haber cierta actividad por parte del titular de los datos para entender que expresa su consentimiento. La exigencia de esta actividad por parte de las normas podría interpretarse como rechazo al silencio, que constituye inactividad, como medio de expresión del consentimiento.

[1668] DEL PESO NAVARRO, *Ley de Protección...,* cit., 2000, p. 21; APARICIO SALOM, *Estudios sobre la Ley…,* cit., 2009, p. 119. SAN 18 de julio 2007, FJ 4: "cuando se acude a la invocación de presunciones, ello equivale a establecer un sistema de suposiciones que pulverizaría esta exigencia esencial del consentimiento, porque dejaría de ser inequívoco para ser "equívoco", es decir, que su interpretación admitiría varios sentidos".

[1669] ZABÍA DE LA MATA, "Principios generales...", cit., 2008, p. 173; SSAN 25 de junio de 2009, FJ 4 y 10 de mayo de 2007, FJ 4.

[1670] Resolución R/01786/2009, de la AEPD, de 24 de julio de 2009, procedimiento PS/00052/2009.

[1671] GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 258.

[1672] DEL PESO NAVARRO, "¿De quién...", cit., 1998.

[1673] CONDE ORTIZ, *La Protección...,* cit., 2005, p. 95; FERNÁNDEZ LÓPEZ, "Principio de consentimiento…", cit., 2010, p. 456: "no toda declaración de voluntad tácita se produce por medio del silencio".

[1674] RUIZ CARRILLO, *Manual Práctico...,* cit., 2005, p. 48.

No obstante, de la propia Ley puede desprenderse también la solución contraria. Y es que en la LOPD cuando se quiere exigir el consentimiento expreso se hace de forma clara[1675]. Se exige el consentimiento expreso para que el tratamiento de los datos denominados sensibles sea posible, lo cual lleva a pensar que en los demás casos cabe la forma tácita. En la normativa europea hay supuestos en que el consentimiento tácito se acepta expresamente[1676]. En el ámbito civil la validez de este tipo de consentimiento también ha sido puesta de manifiesto por la jurisprudencia[1677].

Partiendo de lo que se ha dicho se podría deducir que la LOPD ampara el consentimiento tácito pues éste puede considerarse como inequívoco. La jurisprudencia así parece haberlo entendido desde muy temprano[1678] al igual que la AEPD[1679]. Las posibles dudas sobre la aceptación de este tipo de consentimiento quedan zanjadas actualmente con la aprobación del nuevo reglamento de desarrollo de la Ley. En esta norma, se reconoce expresamente la validez de la autorización tácita, al disponer que el responsable del fichero podrá dirigirse al titular de los datos informándole de los elementos que la Ley exige y señalando que si el titular no responde en el plazo de treinta días se entenderá por consentido el tratamiento[1680].

Lo cierto es que es frecuente encontrarse en la práctica con fórmulas que dan por consentido un tratamiento cuando el titular de los datos no se opone expresamente a dicha manipulación. En estos casos el responsable del fichero llama al titular para que rechace expresamente la posibilidad de que se manipulen los datos relativos a su persona y si este último no se niega a dicho tratamiento se entenderá que consiente esa operación. Realmente, en estos supuestos se puede interpretar que formalmente el consentimiento es inequívoco pues el titular de los datos conoce que el silencio va a conllevar el tratamiento de éstos.

[1675] DAVARA RODRÍGUEZ, *Guía Práctica...,* cit., 2006, p. 73.

[1676] Artículo 4.3.b.ii), Recomendación 97 (18) y Exposición de Motivos del comité de Ministros a los Estados Miembros relativa a la Protección de Datos de Carácter Personal, Recogidos y Tratados con Fines Estadísticos: "*los datos de carácter personal podrán obtenerse y tratarse con fines estadísticos: en la medida en que la Ley lo autorice, y si se hubiere informado a la persona de la recogida o tratamiento de sus datos y no se hubiera opuesto a ello, siempre que el tratamiento no afectare a datos sensibles"*.

[1677] SSTS, 5 de octubre 2007, FJ 2; 31 enero 2007 entre otras.

[1678] Memoria AEPD, 1995: "se distinguen tres modos o formas básicas de otorgar el consentimiento en derecho: expreso, tácito y presunto con plena validez jurídica.
La Sentencia de 8 de febrero de 1964, citada en la de 11 de junio de 1991, de la Sala Civil del Tribunal Supremo establece que <<fuera de los casos en que la Ley exige una declaración expresa, el consentimiento en los negocios jurídicos puede ser prestado en forma tácita; pero en todo caso la declaración de voluntad emitida indirectamente ha de resultar terminante, clara e inequívoca, sin que sea lícito deducirla de expresiones o actitudes de dudosa significación, sino por el contrario reveladoras del designio de crear, modificar o extinguir algún derecho>>, y en la Sentencia de 26 de mayo de 1986 con cita de otras varias, afirma que resulta <<evidente que la reglamentación negocial de intereses puede exteriorizarse a través del comportamiento y existirá declaración de voluntad tácita cuando el sujeto, aun sin exteriorizar de modo directo su querer mediante la palabra escrita y oral, adopta una conducta determinada que al presuponer el consentimiento por una deducción razonable basada en los usos sociales, ha de ser valorada como expresión de la voluntad directa>>"; SAN 13 junio 2007, FJ 3, recientemente admite la validez del consentimiento tácito.

[1679] Informe jurídico, 49/2007 AEPD; Informe jurídico AEPD, 2000, sobre las características que ha de guardar el consentimiento.

[1680] Artículo 14.2 RDLOPD. PUENTE ESCOBAR, "Consentimiento del afectado…", cit., 2009, p. 45.

Si bien se puede asumir que en la norma tiene cabida el consentimiento tácito, se ha de mostrar cierto rechazo, junto a gran parte de la doctrina, a este tipo de prácticas[1681]. Se entiende aquí que el consentimiento constituye un derecho para el titular de los datos de carácter personal, pero también una obligación para el responsable del fichero. Este último tiene la obligación de requerir el consentimiento del afectado y sobre él debe recaer la carga de actuar[1682]. Con la autorización tácita, se invierte esta carga de actuación de forma que es el titular de los datos el que tiene que oponerse al consentimiento[1683]. El hecho de que el silencio del titular favorezca a los responsables de los ficheros que, en muchos casos, son entidades que quieren dar un tratamiento diferente a los datos que ya tienen de los ciudadanos: cesiones de datos, emplear los datos con finalidades distintas a las que motivaron la recogida, etc[1684], es criticable.

La posición que aquí se defiende es más garantista, y favorable al requerimiento en todo caso del consentimiento expreso[1685]. Si la autodeterminación informativa consiste en el control de los datos relativos a uno mismo y el consentimiento constituye el principal instrumento de este control, no es aceptable que el silencio del titular de los datos juegue a favor del responsable del fichero[1686]. Hay que tener presente que en la práctica, muchas veces, el ciudadano no se da cuenta de la existencia de la cláusula que requiere su oposición al tratamiento de los datos, o simplemente por desidia no contesta, lo cual supone la autorización del tratamiento. Que en estos casos se dé por presentada la autorización al responsable del fichero para que manipule los datos de quien permanece en silencio, parece injustificado. Son pues absolutamente loables los intentos que desde diferentes ámbitos se han realizado a lo largo del tiempo para incluir en la definición del consentimiento el calificativo de expreso[1687].

La letra de la Ley actual habrá que entenderla de tal manera que para que el consentimiento tácito sea válido será necesario establecer las garantías suficientes para que el titular de los

[1681] ARENAS RAMIRO, "El Principio del Consentimiento…", cit., 2007, pp. 172-173; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 88; MURILLO DE LA CUEVA, "La Construcción del Derecho…", cit., 2009, p. 59.

[1682] SAN 30 de junio de 2004, FJ 5: "la persona física o jurídica que pretende obtener tal consentimiento deberá arbitrar los medios necesarios para que no quepa ninguna duda de que efectivamente tal consentimiento ha sido prestado".

[1683] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 60; GUICHOT, *Datos Personales...,* cit., 2005, p. 236-237.

[1684] "Diamantes en los ficheros", *El País,* 5 de enero de 2003, las empresas, sobre todo de Marketing Directo, se oponen a que el consentimiento necesario para el tratamiento de los datos tenga que ser expreso, ya que según ellos esto les pondría en situación de desventaja con el resto de Europa. Consideran pues, estas entidades, que el consentimiento puede ser tácito a la vez que inequívoco.

[1685] GONZÁLEZ NAVARRO, "La Relación...", cit., 1999, p. 35: "Ni la Administración Pública ni mucho menos un particular pueden atribuir un valor positivo (de dación de consentimiento) a la falta de respuesta expresa del particular, a menos que la ley lo disponga expresamente. Admitir lo contrario es tanto como dar una patente de corso al responsable del fichero para vulnerar esta exigencia-que es la clave de bóveda de todo el sistema- de la exigencia previa del consentimiento".

[1686] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, pp. 227-232.

[1687] El PSOE propuso que en la definición del consentimiento, junto al calificativo "inequívoco" se establezca el calificativo "expreso". Boletín Oficial de las Cortes Generales, Congreso de los Diputados, nº 278-1, 18 de octubre 2002. Por su parte, la Comisión de Libertades e Informática, propone que se aclare definitivamente lo que se entiende por "inequívoco". En *Navegante* de el Mundo.es, 3 de marzo de 2005, en http://www.elmundo.es/navegante/.

datos tenga conocimiento de los efectos de su silencio[1688]. La propia jurisprudencia ha exigido precaución a la hora de interpretar este tipo de consentimiento, empleando términos que merecen ser reproducidos: este "tema del consentimiento tácito ha de ser tratado con una gran delicadeza cuando están en juego derechos constitucionales básicos (...). En la vida de relación es muy posible reconocer formas de tácita aceptación, pero siempre en aspectos no trascendentales o cuando se está operando sobre situaciones consolidadas y que están en la común consideración a modo de valores entendidos. No es el caso cuando lo que está en juego es la privacidad de las personas. De ahí todas las cautelas normativas tendentes a proteger esa privacidad, sin que quepan interpretaciones de laxitud"[1689]. En esta misma línea, el nuevo reglamento de desarrollo de la LOPD exige también que, a la hora de aceptar el consentimiento tácito como autorización válida, será necesario facilitar por parte del responsable del fichero las posibilidades de actuación o reacción del titular de los datos[1690]. Partiendo, por lo tanto, de la necesidad de exigir gran cautela al admitir el consentimiento tácito como forma de autorizar un tratamiento de datos, la jurisprudencia acaba subrayando que, en todo caso, éste deberá manifestarse a través de actos concluyentes[1691]. El consentimiento tácito, de admitirse, deberá estar bien fundamentado en elementos claramente reconocibles. Así se reconoce también en las resoluciones de la AEPD en las que se exigen ciertas garantías a la hora de aceptar la validez de esta fórmula[1692]. Además, hay que tener en cuenta el problema que plantea este tipo de consentimiento a la hora de probar que ha existido[1693]. Las dificultades a la hora de probar el consentimiento surgen en todos los casos en que éste no haya sido recogido de forma escrita[1694], sin embargo, se agudizan en el caso de la autorización tácita, en la que la inactividad es la base del consentimiento.

[1688] TÉLLEZ AGUILERA, *La Protección...*, cit., 2002, p. 257.

[1689] SSAN, 20 de octubre de 2006, FJ 6 y 21 de enero de 2004, FJ. 4; STSJ Comunidad de Madrid 23 de abril de 2003.

[1690] Artículo 14.4 RDLOPD: "*Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido*".

[1691] STSJ Comunidad de Madrid 30 de enero de 2003, FJ 2, y, en el mismo sentido, STS 8 de febrero de 1964, "fuera de los casos en que la Ley exige una declaración expresa, el consentimiento en los negocios jurídicos puede ser prestado en forma tácita; pero en todo caso la declaración de voluntad emitida indirectamente ha de resultar terminante, clara e inequívoca, sin que sea lícito deducirla de expresiones o actitudes de dudosa significación".

[1692] Resolución 01182/2007, 4 diciembre 2007, procedimiento PS/00178/2007: "el hecho de que la Ley permita el consentimiento tácito no implica que el mismo pueda prestarse sin el cumplimiento de una serie de garantías que aseguren su adecuado conocimiento por el afectado y la posibilidad de aquél de garantizar la negativa a su prestación. Por este motivo, consideramos que no resulta suficiente para considerar tácitamente prestado el consentimiento la mera remisión al afectado de un escrito en que, simplemente, se le informe que, en caso de no obtenerse respuesta del mismo en un determinado plazo, se entenderá que consiente (...).

Ello se funda en que, en caso contrario, no podrá presumirse la existencia del adecuado consentimiento informado al tratamiento ya que, la carga de la prueba en cuanto que la posesión por el titular del fichero de los instrumentos necesarios para acreditar el cumplimiento del deber de recabar ese consentimiento informado constituye una cautela esencial.

En cuanto a la carga de la prueba, la Sentencia de la Audiencia Nacional de fecha 11/05/2001, afirma que "quien gestiona la base, debe estar en condiciones de acreditar el consentimiento del afectado... siendo carga de la prueba del mismo su justificación"".

[1693] DAVARA RODRÍGUEZ, *Guía Práctica...,* cit., 2006, p. 50; ACOSTA RAMÍREZ, "Estudio Práctico…", cit., 2006, p. 276; FERNÁNDEZ LÓPEZ, "Principio de consentimiento…", cit., 2010, p. 461.

[1694] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 121.

En conclusión, el ordenamiento admite tanto la forma oral como escrita del consentimiento. Así mismo, se reconoce la posibilidad de emitir dicha autorización tanto de manera expresa como tácitamente, si bien esta última vía deberá realizarse teniendo presentes ciertas garantías. El consentimiento presunto no tiene cabida en la Ley.

III.3.2.B. La necesidad de que el consentimiento para el tratamiento de los datos de salud sea expreso.

En lo que corresponde a los datos de salud la Ley exige que el consentimiento se dé de manera expresa[1695]. En supuestos específicos, caso de la información derivada de investigaciones biomédicas, principalmente datos genéticos, las leyes exigen que este consentimiento sea, además de expreso, escrito[1696]. Esta exigencia no plantea problemas de interpretación. El legislador, atendiendo a la relevancia que se otorga en general a este tipo de información, ha estimado oportuno que, como punto de partida, el consentimiento para la recogida, tratamiento y cesión de estos datos tenga que ser expreso. No se permite, por lo tanto, que el responsable del fichero pueda deducir o sobrentender, ni siquiera partiendo del silencio del titular de los datos, que este último autoriza la recogida y posterior tratamiento de los mismos. Hay que recordar aquí que, cuando se trata del ámbito sanitario, se ha entendido el concepto de datos de salud en sentido amplio. De esta manera, datos que quizás en otro sector sólo requieren de un consentimiento tácito para su manipulación pueden exigir en estas circunstancias una autorización expresa.

En términos generales, en el ámbito sanitario el consentimiento expreso del titular de los datos para la recogida de los mismos viene dado a través de determinados actos del usuario del sistema sanitario. Cuando éste acude a una consulta y transmite los datos necesarios para que el profesional pueda determinar un diagnóstico se está otorgando el consentimiento para que los datos sean recabados. Y cuando se va a llevar a cabo una operación médica concreta, en el consentimiento informado que el paciente otorga para que dicha operación se pueda realizar se incluye también la autorización para recoger información sobre el estado de salud del paciente. Sería absurdo pensar que se consiente un tratamiento médico determinado y no la manipulación de los datos necesarios para llevar a cabo dicho tratamiento. Esta autorización será suficiente para justificar el tratamiento de datos siempre y cuando se lleve a cabo la previa obligación de informar de forma adecuada y completa. El consentimiento es expreso por cuanto que deriva de un ejercicio activo del titular de los datos, que no deja lugar a dudas sobre su voluntad de que sean recabados con el fin de que puedan ser manipulados para proteger su salud.

La Ley, por lo tanto, exige que el consentimiento sea expreso. No obstante, nada dice en lo que afecta a los datos de salud sobre la necesidad de que sea escrito. Se ha criticado más arriba la regulación que el artículo 7 de la LOPD realiza de los denominados datos sensibles. No se va a reproducir en este momento lo dicho entonces. Basta con decir que no se entiende la razón de ser de la distinta regulación que en los apartados 2 y 3 del precepto de la Ley se realiza de los datos sensibles. Para los datos recogidos en el primero se exige el consentimiento expreso y

[1695] Artículo 7.3 LOPD.
[1696] Artículos 5.2 y 48.1 Ley 14/2007, 3 de julio, de Investigación Biomédica.

escrito, mientras que para los recogidos en el segundo simplemente el consentimiento expreso pero no escrito.

Hay que apuntar que algún Código Tipo ha elevado el nivel de protección de los datos relativos a la salud y ha exigido, cuando menos de inicio, el consentimiento expreso y también escrito para la recogida de este tipo de datos[1697]. También la Ley de Investigación Biomédica exige para algunos casos el consentimiento expreso y escrito de los titulares para que los datos sanitarios puedan ser manipulados. Además, si se entiende que el consentimiento para el tratamiento de los datos puede darse a través del consentimiento dirigido a autorizar una operación médica asistencial, habrá que tener en cuenta que la Ley exige en numerosas ocasiones el consentimiento escrito para llevar a cabo estos actos sanitarios[1698]

Es recomendable, aunque la Ley no exija el consentimiento escrito para el tratamiento de datos de salud, que se recabe de esta manera, pues permite dejar constancia de dicho tratamiento. Lo cierto es que en la práctica, si el consentimiento ha de ser expreso y, además, como prevé la LOPD, tiene que ser inequívoco y específico, la fórmula más adecuada para dejar constancia de que se han cumplido con estas exigencias será la escrita[1699].

III.3.3. Sobre el carácter específico, consciente e informado del consentimiento.

Como tercer requisito se exige que el consentimiento que habilite cualquier tratamiento de datos sea específico, consciente e informado. La LOPD[1700], siguiendo lo dictado por la normativa europea[1701], dispone que la autorización deberá ser específica e informada. Otras normas que entran a regular la figura del consentimiento en otros ámbitos de la vida requieren que sea consciente[1702].

En primer lugar se exige que el consentimiento sea específico. Con esto se quiere decir que ha de ir dirigido a un objeto concreto, esto es, que ha de prestarse sobre un tratamiento en el que todos los términos, en particular la finalidad, estén bien determinados. No son válidos los consentimientos genéricos[1703]. La autorización ha de ser forzosamente explícita, emitida sobre una operación particular de la que se conocen todos los aspectos[1704].

[1697] En el Código Tipo de la Asociación Catalana de recursos asistenciales (ACRA), inscrito en el Registro el 27 de diciembre de 2004, se exige en el artículo 5.3 el consentimiento expreso y escrito para la recogida de los datos relativos a la salud.
[1698] Artículo 8.2 LBAP: "*El consentimiento será verbal por regla general. Sin embargo, se prestará por escrito en los casos siguientes: intervención quirúrgica, procedimientos diagnósticos y terapéuticos invasores y, en general, aplicación de procedimientos que suponen riesgos o inconvenientes de notoria y previsible repercusión negativa sobre la salud del paciente*".
[1699] SAN 16 de febrero de 2008, FFJJ 1 y 3.
[1700] Artículo 3.h) LOPD.
[1701] Artículo 2.h) Directiva 95/46/CE.
[1702] Artículo 3 LBAP: "*Consentimiento informado: la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud*".
[1703] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.
[1704] MURILLO DE LA CUEVA, *Informática y Protección...*, cit., 1993, p. 57.

El consentimiento será específico cuando el sujeto que lo presta lo haga sobre un objeto concreto[1705]. Esta concreción, en el ámbito sanitario, se dará sobre todo cuando las finalidades sobre las que recae quedan definidas de manera clara. Es decir, el usuario del sistema sanitario en el momento en que otorga su autorización para que sus datos de salud sean recabados debe tener claro que la presta para que puedan ser manipulados con determinadas finalidades: asistencia sanitaria directa, investigación, posibles cesiones a organismos como Jueces y Tribunales en determinados casos, etc. La garantía de que el consentimiento va a ser específico se salvaguardará sobre todo con el correcto ejercicio del derecho a la información.

Hay que tener en cuenta que en el ámbito sanitario el consentimiento expreso para la recogida de datos se dará sobre todo a través de determinados actos del usuario, muchas veces dirigidos no tanto a autorizar concretamente el tratamiento de datos sino otras operaciones en las que puede ir implícito el tratamiento de datos. Se hablaba sobre todo del consentimiento para llevar a cabo operaciones asistenciales o para determinar alguna patología o un diagnóstico. En este consentimiento puede verse implícita la autorización para la recogida de datos. No obstante, para que pueda entenderse como específico, el sujeto que lo otorga deberá conocer todos los aspectos que implica la autorización, incluso en lo que concierne a la manipulación de sus datos. Este objetivo se conseguirá a través de la correcta información.

Por otro lado se entiende que el consentimiento ha de ser en todo caso consciente. Esta característica hace referencia a la capacidad de las personas a la hora de otorgar la autorización. El afectado ha de comprender las consecuencias del consentimiento. Ya se ha comentado la posibilidad de representación en los casos de incapacidad y de minoría de edad y a ello nos remitimos.

Por último, la normativa exige que el consentimiento sea en todo caso informado. Se ha analizado en el apartado anterior que para que sea válido es imprescindible que el titular de los datos conozca todos los extremos del tratamiento que va a consentir, pues lo contrario llevaría a un vicio insalvable de la citada autorización. Se apuntó anteriormente que en el CC el "error" invalida el consentimiento[1706].

En materia de protección de datos, para que el consentimiento se invalide por falta de información no es necesario que lo que se omite sea especialmente sustancial, sino que basta con que no se informe sobre alguno de los puntos que recoge la Ley.

En relación a la posibilidad de sancionar la falta de información como vicio del consentimiento otorgado hay que realizar un apunte de interés. En la LOPD la falta de información y la falta de consentimiento se sancionan en preceptos diferentes. Esta circunstancia puede plantear algún problema desde el punto de vista de la aplicación del principio *non bis in idem*[1707], en los casos

[1705] SAN 17 de abril de 2007, FJ 7.
[1706] Artículo 1.266 CC.
[1707] Artículo 133 LPAC: "*No podrán sancionarse los hechos que hayan sido sancionados penal o administrativamente, en los casos en que se aprecie identidad de sujeto, hecho y fundamento*". MESEGUER YEBRA, *El principio "non bis in idem"...,* cit., 2000, p. 13.

en que hay una ausencia de información en los tratamientos en los que el consentimiento informado es requerido.

La falta de información en un tratamiento que la exige es, como no podía ser de otra manera, sancionable[1708]. La falta de consentimiento cuando éste es requerido por la Ley también se sanciona[1709]. Pues bien, como se acaba de ver, el consentimiento, para ser válido, necesita de la información. Sin información no hay consentimiento. Así, ¿la falta de información, puede conllevar una doble sanción: una por incumplir el deber de informar, y otra por incumplir el deber de obtener el consentimiento del titular de los datos? ¿Puede el mismo hecho acarrear esa doble sanción? Esta pregunta lleva a plantear la aplicabilidad de la figura del *non bis in idem.* No se pretende ahora un estudio sobre la aplicación del principio citado, fundamentalmente, porque todavía hoy su interpretación no resulta nada pacífica[1710].

La aplicación del principio citado se da, en líneas generales, para evitar que un sujeto pueda ser sancionado dos veces por el mismo hecho, basándose en el mismo fundamento y para salvaguardar el mismo interés jurídico[1711]. Se ha considerado que es necesario, para la aplicación del *non bis in idem*, que se dé la que se ha denominado "triple identidad"[1712]: de sujeto, de hecho y de fundamento. En el caso que aquí se trata se encontraría un único sujeto, el responsable del fichero, que lleva a cabo una acción, no otorgar la información oportuna al titular de los datos, pero que puede acarrear una doble consecuencia jurídica o sanción. La clave, en este caso, está en determinar si es posible aplicar fundamentos jurídicos distintos al hecho sancionable a la hora de llevar a cabo la doble sanción. Si una misma acción puede ser sancionada atendiendo a diferentes fundamentos jurídicos, que protegen intereses o bienes diferentes, la doble sanción será posible[1713].

En el caso que aquí se plantea, si se atiende a la Ley, la falta de información y la falta de consentimiento se regulan en apartados diferentes con consecuencias jurídicas distintas. Por lo tanto, ambos hechos, a pesar de derivar de una misma actuación del responsable del fichero, podrían ser sancionados atendiendo a fundamentos jurídicos diferentes. En algún caso la AEPD parece haber aplicado este concurso real, interpretando que ambas sanciones han de ser ejecutadas completamente frente al responsable del fichero por ambos incumplimientos, a pesar

[1708] Artículo 44.2.d) LOPD: "*Son infracciones leves: d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley*"; artículo 44.3.l), LOPD: "*Son infracciones graves: l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado*".

[1709] Artículo 44.4.c) LOPD: "*Son infracciones muy graves: c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7*".

[1710] MESEGUER YEBRA, *El principio "non bis in idem"...,* cit., 2000, p. 9; GALLARDO CASTILLO, *Los Principios...,* cit., 2008, pp. 289-314; CUBERO MARCOS, *El principio…,* cit., 2010, p. 31.

[1711] ALARCÓN SOTOMAYOR, *La garantía non bis in idem…,* cit., 2008, p. 23; CUBERO MARCOS, *El principio…,* cit., 2010, p. 27 y siguientes.

[1712] SSTC 16 de enero de 2003, FJ 5; 7 de julio de 2005, FJ 2.

[1713] LASAGABASTER HERRARTE, "Non bis in idem...", cit., 2006, p. 293; ALARCÓN SOTOMAYOR, *La garantía non bis in idem…,* cit., 2008, p. 47.

de que la falta del consentimiento se fundamente en el hecho de que no se ha dado la debida información[1714].

No se comparte esta solución. Si bien es cierto que no se está ante un caso de *non bis in idem*, pues el fundamento jurídico que se aplica a la hora de sancionar es distinto por la falta de información y por la falta de consentimiento, la solución no debe ser la aplicación de ambas sanciones. Se interpreta que se está ante un supuesto de concurso medial, en el que una infracción constituye el medio para alcanzar la otra[1715]. En el caso que se estudia, la falta del consentimiento no se da sin la falta de información. Es la ausencia de esta última la que lleva a la primera infracción. Para estos supuestos señalan las normas que "*cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida*"[1716]. En la CAPV, el ordenamiento determina que "*si la pluralidad de infracciones proviniese de un solo hecho o de varios realizados aprovechando idéntica ocasión, o una de las infracciones fuese medio necesario para la comisión de otra y, atendidas las circunstancias del caso, ello manifestara una menor reprochabilidad en la conducta del responsable, la regla establecida en el número precedente*[1717] *se aplicará imponiendo las sanciones menos graves de las establecidas para cada infracción*"[1718].

III.3.4. Sobre el carácter previo del consentimiento.

Por último, hay que analizar un requisito que si bien no se recoge expresamente en las definiciones de las normas, es de gran importancia. Se trata de la necesidad de que el consentimiento del titular de los datos sea previo al tratamiento de los mismos. El artículo 6 de la Ley no dice nada al respecto. No obstante, atendiendo al conjunto del texto legal puede deducirse claramente la necesidad de que el consentimiento sea previo.

La regulación relativa a la cesión de datos exige que el consentimiento del titular preceda en todo caso a la comunicación, y aunque lo previsto para las comunicaciones de los datos no puede aplicarse por analogía para todos los tratamientos, da una indicación de cuál puede ser la voluntad del legislador al respecto.

A pesar del silencio de la LOPD ha habido autores que, basándose en el artículo 5.4 de la Ley, han considerado la posibilidad de iniciar un tratamiento de datos de carácter personal sin el consentimiento del titular de los datos. Se ha asumido por esta línea doctrinal la viabilidad de que

[1714] Resolución AEPD, R/00677/2005, 2 julio de 2007, procedimiento nº AA.PP/00095/2006: "no se les informó en los cuestionarios en los que se recababan los datos de los extremos del artículo 5.1 de la LOPD, por lo que, cabe concluir que el Servicio Andaluz de Salud no contaba con el consentimiento "*expreso"* para el tratamiento de datos "*especialmente protegidos".*

[1715] ALARCÓN SOTOMAYOR, *La garantía non bis in idem…,* cit., 2008, p. 77; CUBERO MARCOS, *El principio…,* cit., 2010, p. 78.

[1716] Artículo 4.4 RD 1398/1993, 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora.

[1717] Artículo 17.1 Ley 2/1998, 20 de febrero, de la Potestad Sancionadora de las Administraciones Públicas de la Comunidad Autónoma Vasca: "*Al responsable de dos o más infracciones se le impondrán todas las sanciones correspondientes a las diversas infracciones*".

[1718] Artículo 17.2 Ley 2/1998, 20 de febrero. Al respecto, LASAGABASTER HERRARTE, "Non bis in idem...", cit., 2006, pp. 265-300.

este consentimiento se emita una vez iniciado el tratamiento[1719]. Como ya se dijera, en este artículo se reconoce la posibilidad de prorrogar el deber del responsable del fichero de informar al titular de los datos sobre los puntos que exige la Ley durante un plazo máximo de tres meses, en los supuestos en que los datos de carácter personal son recabados de fuente distinta al titular. Según la citada doctrina, la fuente distinta al titular de los datos los transmitiría al responsable del fichero en una especie de acto previo que luego ratificaría el titular de los datos con su consentimiento. Esto es, se estaría ante una especie de representación *sui generis*: el tercer sujeto actuaría como representante del titular de los datos llevando a cabo un acto, la transmisión de los datos al responsable del fichero, que posteriormente ratificará el titular de los mismos[1720].

La interpretación que aquí se realiza a este respecto es diferente. Como se ha expuesto en anteriores apartados, en el artículo 5.4 LOPD se reconoce una prórroga al ejercicio del derecho a la información, prórroga en la que el responsable del fichero podrá tratar los datos relativos a una persona a la que, sin embargo, deberá informar lo antes posible y en un plazo máximo de tres meses. Se concluía entonces que este precepto se refiere a los supuestos en que el consentimiento está exceptuado. Sin información no cabe consentimiento y si la información se prorroga, se prorrogaría también automáticamente el consentimiento. No se puede aceptar, sin embargo, que el consentimiento se prorrogue si no hay una previsión normativa que lo justifique. Si un tratamiento requiere del consentimiento del titular, se entiende que este tratamiento no podrá iniciarse sin la autorización del titular. Cuesta encontrar base alguna para justificar el

[1719] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, p. 221: "Respecto del carácter previo del consentimiento, ya hemos visto que se trata de un requisito específico de las cesiones de datos, que no se menciona en el artículo 6 respecto de las operaciones de tratamiento. La mayor peligrosidad que generan los actos de cesión justifica una mayor exigencia respecto de éstas. No obstante, nos plantea serias dudas el silencio del artículo 6, dudas sobre la admisibilidad de que el afectado consienta con posterioridad (p. 222) a las operaciones de tratamiento que no son cesión. En cualquier caso, tal posibilidad se deduce implícitamente del artículo 5.4 (...)
si los datos ya han sido recabados de otra persona, permitiéndose la remisión de información en un momento posterior, se deduce que el consentimiento del afectado concurre en un momento posterior al tratamiento. No pensamos que se pueda alegar que lo que este precepto afirma es que, si bien se informa y recaban los datos inicialmente, se suspende el tratamiento hasta la concurrencia del consentimiento, pues entonces no tendría sentido la finalidad de agilidad y rapidez que manifiesta el artículo 5.4 y si los responsables de los ficheros estuvieran supeditados a tal circunstancia, en la práctica se dirigirían directamente al afectado.
¿Qué calificación puede recibir este supuesto de consentimiento posterior a las operaciones que pretende legitimar? No nos encontramos ante un supuesto de condición suspensiva, puesto que la misma puede consistir en un suceso, un hecho o acto, pero en modo alguno se puede considerar condición uno de los elementos esenciales como es el consentimiento, pues ello supondría la inexistencia de aquél, no la suspensión de su eficacia (...).
p. 223: Por otra parte, no entendemos que, dada la trascendencia de la voluntad del afectado, como esencial del derecho a la Autodeterminación informativa, según vimos en el epígrage anterior, la LOPD pueda establecer tal diferencia de régimen según los actos de que se trate. El control sobre los datos no puede posponerse a un momento en el que seguramente ya se hayan producido operaciones de tratamiento (...).
En realidad, la solución al problema del consentimiento posterior al tratamiento de datos puede venir de la mano de otra figura tradicional del Derecho Civil: la representación (...) el artículo 5.4 de la LOPD admite la posibilidad de que los datos se recaben de persona distinta del afectado (...).
Se trata de un supuesto en el que dicho sujeto realiza un acto que produce efectos jurídicos en la esfera del afectado como si de un negocio representativo se tratara. No obstante, se trata de una actuación sin poder, pues en caso contrario no sería necesario que el afectado manifestara después su voluntad. Por lo tanto, la exigencia del consentimiento en un momento posterior juega un papel de la ratificación de los actos realizados (...).
p. 224: "En tal sentido se pueden interpretar los términos empleados al respecto por Aparicio Salom. Según este autor, la exigencia del plazo de tres meses del artículo 5.4 de la LOPD trae como consecuencia que durante este plazo el tratamiento será lícito y, una vez satisfecha la obligación de información, el tratamiento es válido".

[1720] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, pp. 221-225; APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, pp. 66-68.

retraso en la solicitud del consentimiento, cuando éste es requerido por la Ley. Así lo ha admitido también la jurisprudencia[1721]. Cosa distinta será que se encuentren motivos que justifiquen la excepción al derecho a otorgar el consentimiento.

Se ha subrayado que el consentimiento es una de las piezas centrales que configuran el derecho a la autodeterminación informativa, pues supone la principal facultad de control sobre los datos concernientes a una persona. Partiendo de esta idea, es difícil justificar que se pueda iniciar la manipulación de unos datos sin la autorización requerida por la Ley sin que haya excepción alguna a dicho derecho.

En el ámbito sanitario, en los casos en que el consentimiento no está exceptuado, la necesidad de que éste sea previo al tratamiento es evidente. En la práctica no parece que este requisito plantee mayores problemas. Como se ha apuntado, esta autorización se da, en la mayoría de los casos, cuando el paciente transmite directamente los datos al profesional sanitario o cuando facilita su cuerpo para ser fuente de información. El consentimiento resulta implícito en esa misma transmisión de los datos del paciente al profesional sanitario.

Podrían encontrarse en este ámbito situaciones en que la prórroga a la hora de otorgar el consentimiento tuviera sentido. Pueden darse circunstancias en las que el paciente esté en una situación en que le sea imposible llevar a cabo el consentimiento con todas las garantías exigidas: inconsciencia, enajenación transitoria, etc. En estos casos cabría plantearse la posibilidad de aplicar una prórroga en la ejecución de la autorización por parte del titular de los datos. El paciente daría su autorización cuando recuperara las facultades para ello. Cabría también la posibilidad de ejecutar el consentimiento a través de familiares o representante.

Sin embargo, lo cierto es que en estos casos más que de prórrogas y alternativas en la forma de autorizar un tratamiento habrá que hablar de la posibilidad de exceptuar el derecho a consentir. Como se verá a continuación, el hecho de que la salud de un individuo esté en juego puede exceptuar la necesidad de requerir su consentimiento para el tratamiento de los datos. La norma no parece apostar por la vía de la prórroga, sino por la aplicación de la excepción. Esta regulación tiene sentido en los siguientes términos: la justificación de la aplicación de un límite viene motivado no por la existencia de dificultades para recabar la autorización, sino debido a que se entiende que existe una causa fundada para no someter el tratamiento de los datos a la voluntad de su titular. Se interpreta que existe un bien jurídico cuya protección resulta de mayor importancia. En el ámbito sanitario, la excepción al derecho a consentir se justifica no porque se den situaciones en que la obtención de dicha autorización resulte complicada, sino porque se entiende que la protección de la salud de los individuos es más relevante jurídicamente que la salvaguarda de su derecho a la autodeterminación informativa.

[1721] SAN 8 febrero 2002, FJ 3: "En primer lugar ha de decirse que el consentimiento para el tratamiento de datos de carácter personal que exige el art. 6.1 de la Ley 5/92, es un consentimiento previo, que no puede ser convalidado por el posterior que efectúe el afectado, de forma que la conducta infractora se habrá cometido si el tratamiento de datos se realiza sin el necesario consentimiento de la persona de que se trate. El consentimiento posterior del afectado una vez que ha tenido lugar el tratamiento, no es una circunstancia que haga desaparecer la infracción misma, porque la conducta del sujeto es la descrita en el tipo establecido por la norma, y como tal ha de reputarse típicamente antijurídica, es decir, se ha cometido la acción descrita en el tipo infractor".

III.4. Excepciones al consentimiento en el tratamiento de datos sanitarios.

III.4.1. Consideraciones previas.

Uno de los aspectos más problemáticos en relación al tratamiento de los datos sanitarios es sin duda el análisis de las excepciones que la normativa recoge a la obligación de recabar el consentimiento para la manipulación de los datos.

Hay que empezar apuntando que la Directiva y la LOPD parten de fundamentos diferentes a la hora de limitar el derecho a consentir el tratamiento de datos sanitarios. La norma europea, en lo que respecta a los datos de especial sensibilidad, entre los que se encuentran los relativos a la salud, parte de la siguiente consideración: *"los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad"*[1722]. Si bien es cierto que en esta norma se establecen diferentes supuestos en que se permite el tratamiento de los citados datos sensibles, es significativo que el punto de partida sea la prohibición de su manipulación[1723]. Este hecho da a entender la especial importancia de la información que revelan los datos que se enumeran en dicho artículo, entre los que están los de salud[1724].

En esa misma línea la regulación de la norma europea va más lejos. Teniendo en cuenta la importancia del contenido de los denominados datos sensibles, en la Directiva se recoge la posibilidad de que el consentimiento del titular no sea suficiente argumento para permitir el tratamiento de los denominados datos sensibles. Se reconoce a los Estados miembro la alternativa de disponer en su regulación interna que el consentimiento del titular no sea suficiente para levantar la prohibición de manipular los citados datos sensibles[1725]. Se desprende de esta redacción la idea de que puede encontrarse un tipo de información sobre la que ni siquiera su titular puede disponer como quiera.

Siguiendo esta línea interpretativa, y haciendo referencia precisamente al ámbito de los datos sanitarios, el Consejo de Europa reconoce que la figura del consentimiento otorga una protección menor a este tipo de datos que la que otorgan las obligaciones legales[1726]. Es evidente que la prohibición legal de tratar una serie de datos, entre los que se encuentran los sanitarios, constituye una protección inquebrantable. La letra de la Ley no puede incumplirse. Por el

[1722] Artículo 8 Directiva 95/46/CE.
[1723] ELIAS BATURONES, "La Regulación...", cit., 1998, p. 1.232.
[1724] Documento de Trabajo, del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.
[1725] Artículo 8.2.a) Directiva 95/46/CE: "*lo dispuesto en el apartado 1 no se aplicará cuando: a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado*"
[1726] Punto 83 Memoria explicativa de la Recomendación R (97) 5 del Consejo de Europa: *"Apart from any legal provision or obligation, medical data may also be collected and processed if the data subject .or his/her legal representative- has given consent, unless domestic law opposes this. The drafters of the recommendation were aware that, from the point of view of protection of medical data, consent of the data subject gives fewer guarantees than legal obligations or legal provisions which –by virtue of article 6 of the convention- should be accompanied by appropriate safeguards (...)".*

contrario, el consentimiento del titular de los datos supone una garantía que puede salvarse, pues la voluntad del afectado es manipulable. En algún caso se ha entendido que por la vía del consentimiento puede llegar a darse una renuncia del derecho a la autodeterminación informativa en ámbitos como el laboral, en que el titular de los datos puede estar, en cierto sentido, desprotegido[1727].

Ciertamente, podría considerarse paternalista lo que plantea la regulación europea minimizando el valor del consentimiento del titular de los datos. Incluso podría entenderse como vulneradora de la autonomía del ciudadano, pues una cosa es que atendiendo a un bien jurídico que se considera superior se exceptúe el consentimiento del titular de los datos, y otra que se interprete que el ciudadano es incapaz de proteger por sí mismo con eficacia la información relacionada con él. Sin embargo, si bien una prohibición como la que habilita la norma europea puede resultar de inicio exagerada, si se atiende a la realidad puede apreciarse que la falta de concienciación de la ciudadanía respecto a la materia que aquí se trata podría venir a justificar medidas como la planteada por la Directiva[1728].

En la LOPD no se ha recogido con carácter general la posibilidad de prohibir el tratamiento de los datos denominados sensibles. En el ámbito estatal, por lo tanto, y salvo en un supuesto determinado[1729], el punto de partida para el tratamiento de los datos sanitarios no es su prohibición, sino el consentimiento del titular. En este sentido, el espíritu de la Ley es que todo tipo de dato, incluso el relativo a la salud, pueda ser manipulado si media el consentimiento del titular. Esta facultad de autorizar el tratamiento se erige, por lo tanto, en garantía principal del derecho a la autodeterminación informativa. En principio será necesaria la autorización expresa del titular para que esta información sea manipulada. Luego la Ley prevé una serie de supuestos en que esta facultad de consentir se encontrará exceptuada.

Las excepciones que la LOPD dispone a la faculta de consentir son múltiples. Según el artículo 6.2 *"no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado".*

[1727] GOÑI SEIN, *La Videovigilancia...,* cit., 2007, p. 102.

[1728] Es especialmente significativo el caso de los trabajadores de una empresa londinense que revelaron la contraseña de su ordenador a cambio de una barra de chocolate, y sus datos personales a cambio de participar en un sorteo de dos entradas para el teatro. Noticia publicada en *El Mundo*, de 10 de abril de 2005.

[1729] Artículo 7.4 LOPD: "*Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual*". Lo que está vetado en la Ley es un uso concreto de estos datos: el catalogar a las personas en base a este tipo de información. Pero estos datos pueden ser empleados cuando la finalidad lo justifique.

Las excepciones recogidas en el citado artículo atienden al régimen general que esta norma reconoce para todo tipo de datos. Evidentemente éstas no pueden aplicarse directamente a los datos sanitarios que siendo sensibles son objeto de una mayor protección por parte de la Ley, debiendo acudir a los artículos 7.3, 7.6 y 8 de la Ley, que más adelante se analizarán y que se refieren particularmente a los datos sanitarios. Sin embargo, si bien las excepciones al consentimiento cuando se trata de datos relativos a la salud se fijan en estos últimos artículos, habrá que tener en cuenta también lo señalado en el artículo 6, pues reconoce una serie de límites que pueden tener cierto interés para comprender mejor las excepciones al consentimiento en el tratamiento de los datos sanitarios.

El hecho de que la Ley haya dispuesto una batería de límites al derecho a consentir no es en principio criticable. Cierto es que este derecho se basa en la capacidad de control del titular de los datos y que de alguna manera los datos son propiedad del titular de los mismos[1730], pero es sabido que no hay derecho absoluto alguno y que también la capacidad de controlar los datos debe contar con limitaciones en el ordenamiento[1731]. Sin embargo, desde ahora hay que poner en tela de juicio el sistema de límites al consentimiento que dispone la Ley. Como subraya la mayor parte de la doctrina, este grupo de excepciones plantea un problema de envergadura. Al igual que ocurría en el derecho a ser informado, el alcance de las excepciones que establece la LOPD al principio del consentimiento es excesivamente amplio. Según la mayoría de autores dichos límites vacían de contenido la facultad de consentir, ya que son muchos y se encuentran formulados con tal grado de indeterminación que hacen que el derecho a consentir el tratamiento de los datos de carácter personal acabe siendo impracticable[1732]. Se podría afirmar que la especial importancia que se atribuía al comienzo de este apartado al derecho al consentimiento se ve diluido con la fijación en la Ley de las excepciones que recoge y que ahora se van a analizar[1733].

III.4.2. Excepción al consentimiento en la manipulación de los datos de carácter personal por la Administración pública.

Dispone la LOPD que *"no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en*

[1730] *Manifiesto en Defensa de la Confidencialidad y el Secreto Médico*, aprobado en Madrid, en junio de 2003, en el punto 3º, se afirma que "los datos médicos pertenecen a cada paciente, y éste tiene los derechos sobre los mismos. El profesional sanitario a quien el paciente se los confía actuará como depositario ejerciendo esos derechos como agente y responsable ante el paciente". Por su parte, el HIGH LEVEL COMMITTEE ON HEALTH, en su *Health Telematics Working Group of the High Level Committee on Health: Final Report*, de abril de 2003, p. 9, afirma también que el concepto de paciente como propietario de los datos es una idea o principio del que hay que partir. Como apunta PIÑAR MAÑAS, prólogo a la obra de DE MIGUEL SÁNCHEZ, *Tratamiento de Datos...*, cit., 2004, p. 14, "sigue siendo usual que se piense que el "propietario" de los datos que se recogen en un fichero es el titular del fichero y no las personas a las que los datos en él contenidos se refieren".

[1731] PÉREZ LUÑO, "La Defensa...", cit., 1986, p. 45, comentando la ya citada sentencia del Tribunal Federal Alemán sobre la Ley del Censo de Población, subraya que el "ciudadano de un Estado social de Derecho no tiene un derecho sobre <<sus>> datos, en el sentido de una soberanía absoluta e ilimitada, sino que es una persona que se desenvuelve en una comunidad social en la que la comunicación y la información resultan imprescindibles".

[1732] OROZCO PARDO, "La Protección...", cit., 2002, p. 189; CASTELLS ARTECHE, "Derecho a la Privacidad...", cit., 1994, p. 255; HERRÁN ORTIZ, *El Derecho...,* cit., 2003, pp. 57-58; PRIETO GUTIÉRREZ, "La Directiva...", cit., 1998, p. 1.105.

[1733] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 177.

el ámbito de sus competencias". Añade el Reglamento de desarrollo de la LOPD, que esta excepción al consentimiento entrará en juego cuando el tratamiento de datos se lleve a cabo en desarrollo de las competencias atribuidas a la Administración por una norma con rango legal o una norma de Derecho comunitario[1734]. La excepción está en principio plenamente justificada. Las administraciones, para llevar a cabo los fines que les han sido asignados por el ordenamiento y en el marco de sus competencias, podrán manipular los datos de carácter personal de los ciudadanos sin necesidad de requerir el consentimiento de los mismos. Parece oportuno, sin embargo, hacer algún apunte sobre su contenido a la luz de un análisis comparativo entre la norma estatal y otras normas.

En primer lugar hay que hacer una breve mención al contenido de la Ley Vasca de protección de datos. La fórmula empleada por la norma autonómica es prácticamente la misma a la utilizada en la Ley estatal[1735]. La primera también reconoce la excepción dispuesta por la norma estatal pero añade que la excepción será efectiva *"salvo precepto legal en sentido contrario"*. La Administración podrá manipular los datos de los ciudadanos sin el consentimiento de éstos, salvo que una Ley establezca lo contrario. Por lo tanto, en la norma autonómica cabe la posibilidad de que una Ley requiera el consentimiento del titular de los datos para el tratamiento de los mismos cuando vayan a ser manipulados por la Administración. Se trataría de la excepción a la excepción al consentimiento. En la LOPD no se recoge esta posibilidad.

Se entiende aquí que la previsión de la Ley vasca es acertada. Si una norma con rango legal puede excepcionar el consentimiento, otra norma con el mismo rango también podrá exigirlo. Esta posibilidad abre la puerta a que el respeto al derecho a la autodeterminación informativa sea absoluto cuando los datos de carácter personal sean manipulados por las administraciones. Hay que valorar positivamente la alternativa que reconoce la Ley autonómica, teniendo en cuenta que lo que justifica la excepción al consentimiento cuando los datos son empleados por la Administración no es otra cosa que la defensa, por este último, del interés general. La valoración positiva se justifica por el hecho de que en la realidad podrán reconocerse supuestos en que en la actividad de la Administración sea complicado identificar el interés general[1736]. En estos casos es más que recomendable que incluso el aparato público tenga que exigir el consentimiento del

[1734] Artículo 10.3 RDLOPD: "*Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando: a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de Ley o una norma de Derecho comunitario*". ARROYO YANES, "Las Administraciones Públicas….", cit., 2010, p. 544, pone de manifiesto cómo se produce la relación entre la LOPD y el RDLOPD que la desarrolla, en la medida en que la disposición general incorpora una regulación más amplia que la Ley, que quizá tenga dudoso encaje en una norma con rango reglamentario, por referirse a cuestiones muy cercanas al contenido esencial del derecho a la autodeterminación informativa.

[1735] Artículo 5 Ley Vasca 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos: *"Las administraciones públicas y demás instituciones, corporaciones y entidades a que se refiere el artículo 2.1 de esta ley sólo podrán recoger datos de carácter personal para su tratamiento cuando sean adecuados, pertinentes y no excesivos para el ejercicio de las respectivas competencias que tienen atribuidas. Salvo precepto legal en sentido contrario, para la obtención de dichos datos no será preciso recabar el consentimiento de los afectados, pero sólo podrán utilizarse para las finalidades determinadas, explícitas y legítimas para las que se hubieran obtenido, sin perjuicio de su posible tratamiento posterior para fines históricos, estadísticos o científicos, de acuerdo con la legislación aplicable"*.

[1736] Más aún hoy día que "la huída del Derecho Administrativo" se plantea como uno de los principales problemas a los que se enfrenta la ciencia jurídica.

titular de los datos para la manipulación de los mismos, en la medida en que no se encuentra un bien jurídico suficiente que justifica la excepción[1737].

En segundo lugar hay que detenerse en la observación de la normativa supranacional. Atendiendo a la redacción de la norma estatal parece que para la Administración la excepción al consentimiento se convierte en regla general[1738]. En el marco de las funciones que el ordenamiento le designa cada órgano administrativo puede manipular los datos de los ciudadanos sin el consentimiento de éstos. Esta regulación fue criticada con prontitud en comentarios a la Ley de protección de datos de 1992[1739]. Ciertamente, no parece que pueda asumirse como punto de partida una regulación tan generosa con respecto al derecho a otorgar el consentimiento.

Este principio ha de limitarse en algún sentido y para ello hay que acercarse a lo que dispone el ordenamiento supranacional. Según la Directiva europea el tratamiento de los datos de carácter personal por parte de la Administración podrá llevarse a cabo sin el consentimiento del titular, cuando sea necesario para la defensa o la promoción del interés público[1740]. Sin duda alguna, la referencia a este interés público hay que entenderla aplicable al límite que se comenta. Es precisamente este fin el que justifica la excepción[1741]. El límite al derecho a la autodeterminación informativa tiene sentido en la medida en que se persigue un bien jurídico digno de protección, como puede ser este interés público. El problema reside en determinar lo que hay que entender por interés público[1742]. La jurisprudencia viene admitiendo el carácter de concepto indeterminado de esta expresión[1743]. Las interpretaciones que se pueden hacer del

[1737] No se entienden las críticas vertidas a este precepto de la Ley Vasca de Protección de Datos, en el sentido de considerarla menos protectora que la LOPD estatal. El Diputado MACHÍN EXPÓSITO, entendía que la Ley vasca daba la vuelta a lo dispuesto en la LOPD con respecto al consentimiento. Según MACHÍN la Ley vasca viene a posibilitar que se puedan tratar datos de carácter personal sin el consentimiento, a no ser que una Ley establezca lo contrario: la regla general es tratar sin consentimiento, y la excepción es el consentimiento (Diario de Sesiones del Parlamento Vasco, nº 91, 25 de febrero de 2004). Nada más lejos de la realidad. Hay que tener en cuenta que la Ley vasca se refiere a los datos empleados por la Administración, y que para el tratamiento de los datos por esta institución no se exige el consentimiento. En este sentido, la Ley vasca y la LOPD disponen lo mismo. Lo único que hace la Ley Vasca es fijar la posibilidad de que una Ley venga a exigir dicho consentimiento incluso para el caso en el que los datos sean tratados por una Administración.

[1738] GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 262.

[1739] ORTI VALLEJO, "Cinco años...", cit., 1997.

[1740] Artículo 7.e) Directiva 95/46/CE: "*Los Estados miembros dispondrán que el tratamiento de datos personales sólo puede efectuarse si:*
e) es necesario para el cumplimiento de una misión de interés público o inherente al responsable del tratamiento o a un tercero a quien se comuniquen los datos".

[1741] PÉREZ VELASCO, "Los ficheros...", cit., 2006, p. 118; APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 139.

[1742] PRIETO GUTIÉRREZ, "La Directiva...", cit., 1998, p. 1.106; ELIAS BATURONES, "La Regulación...", cit., 1998, p. 1.226.

[1743] STS 22 de junio de 1999, FJ 2: "La reiterada alegación que en el escrito del recurso de casación se hace al concepto de interés público, como directamente vulnerado, se integra en lo que constituye un concepto jurídico indeterminado: «interés general», aduciéndose la falta de razones determinantes de la concesión del aplazamiento en la cuestión examinada.
El interés público cumple una doble función en relación con la actividad administrativa, puesto que opera, de una parte, como factor de aplicación del derecho público, y es criterio determinante de la competencia de este Tribunal y de otra parte, opera como factor de legalidad de la actividad administrativa, esto último relacionado con la invocación de preceptos constitucionales que se contienen en el escrito de interposición del recurso de casación, en donde se

mismo son múltiples. Sin embargo, parece que en la voluntad del legislador europeo está el comprender este concepto en sentido estricto, limitándose a las funciones de carácter eminentemente públicas en que se defiende el interés general[1744].

No toda la actividad administrativa justifica el tratamiento de los datos de carácter personal sin el consentimiento del titular. Tendrá que ser una actuación en la que la Administración esté representando el interés general y proteja valores o intereses de suficiente envergadura como para anteponerse a un derecho fundamental[1745]. Sólo en estos casos, y siempre que actúe dentro del ámbito de sus competencias y para el cumplimiento de los fines que les han sido asignados por una Ley o por norma de Derecho comunitario[1746], podrá justificarse el límite a la facultad de consentir del titular de los datos.

Dentro de los márgenes que se acaban de señalar es jutificable que la Administración cuente con esta facultad a la hora de tratar información de carácter personal. Y es que lo contrario podría poner en peligro la efectividad de la actuación del aparato público. Es de considerar que la actividad administrativa se basa en un continuo manejo de este tipo de datos. Así, la exigencia de que en cada operación que vaya a realizar con dicha información tenga que cumplir estrictamente con las garantías que prevé la LOPD, supone una carga excesiva que podría dificultar sobremanera el funcionamiento ágil de la Administración[1747]. Además, el dejar a la voluntad de los particulares el correcto funcionamiento de la Administración conllevaría que se sometiera a la conformidad de cada ciudadano la realización del interés general o público. Aquí reside la justificación de la excepción al consentimiento.

Como se ha dicho, esta excepción no tiene aplicación cuando se trata de manipular datos relativos a la salud, cuyo tratamiento se sujeta a un régimen específico que se verá más adelante. Si la excepción tuviera aplicación en este ámbito, se entendería que la Administración podría manipular los datos de los usuarios sin necesidad de recabar su consentimiento para ello. Parece excesivo pensar que de inicio este tipo de información pueda ser manipulada por cualquier órgano administrativo en el ejercicio de sus funciones sin necesidad de recabar la

aduce, expresamente, la interdicción de la arbitrariedad de los poderes públicos y el artículo 103, en donde se contienen los principios esenciales de legalidad de la actividad administrativa".

[1744] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 71, apunta que "el interés público a que se refiere la Directiva debe entenderse en el sentido más limitado, como aquél que ostentan las administraciones como responsables de la gestión de aquellas actividades que, no pudiendo ser atendidas por los ciudadanos, se reservan en exclusiva al poder público, atribuyéndole potestades excepcionales de supremacía para garantizar el éxito de las mismas. Deben excluirse, por ello, aquellas actividades que se desvinculan de las potestades públicas y se identifican con las actividades que se desarrollan de forma idéntica por los particulares"; SERRANO PÉREZ, *El Derecho Fundamental...*, cit., 2003, p. 212: "A nuestro modo de ver la Directiva europea no contiene una alusión a toda la actuación de la Administración o de los poderes públicos, sino solamente a una función o actividad precisa y limitada que, al amparo de un interés público, requiera suprimir el consentimiento para realizarse con eficacia y en aras del citado interés".

[1745] STC 17 de febrero de 1984, FJ. 3.

[1746] COLLADO GARCÍA-LASARA, *Protección de Datos...*, cit., 2001, pp.20-21; ARROYO YANES, "Las Administraciones Públicas…", cit., 2010, pp. 545-546, se niega la posibilidad de que la excepción al consentimiento opere cuando las competencias a la Administración en cuestión haya sido atribuidas por norma distinta a la Ley o norma de Derecho Comunitario.

[1747] VALERO TORRIJOS y LÓPEZ PELLICER, "Algunas Consideraciones...", cit., 2001, pp. 260-261.

autorización del titular. Resulta lógico pensar que no toda actividad administrativa puede justificar un tratamiento de datos de salud sin consentimiento del titular.

Hay que resaltar que en el ámbito sanitario la excepción al consentimiento se reconoce no porque sea la Administración la que lleve a cabo el tratamiento de los datos, sino porque la finalidad que se persigue con la manipulación de los mismos no es otra que proteger la salud de las personas. Se limita el derecho a la autodeterminación informativa, porque la Administración persigue un interés concreto, a saber: la salvaguarda de la salud. Es la finalidad, no el sujeto, la que justifica la excepción. Independientemente de que dicha finalidad sea llevada a cabo por la Administración o no, el carácter fundamental de la misma no varía. Es por ello que la doctrina ha entendido que la excepción al consentimiento es aplicable tanto en el caso de los centros públicos como privados[1748].

En términos generales el buen funcionamiento de la Administración sanitaria en la realización de sus competencias exige que no se requiera la autorización de los usuarios para manipular sus datos de salud. La necesidad, por ejemplo, de que la transmisión de estos datos entre órganos de un mismo centro o entre diferentes centros se dé de manera rápida y ágil hace que no sea exigible el consentimiento del titular en cada acto que haya de llevarse a cabo con los datos.

Es precisamente porque lo relevante a la hora de aplicar la excepción es la finalidad que se persigue con la utilización de los datos, por lo que resulta necesario analizar más detenidamente los artículos 7 y 8 que más adelante se verán, que en el genérico artículo 6 que ahora se comenta brevemente. Si bien la aplicación de este último en el ejercicio de la Administración sanitaria podría tener sentido, el ordenamiento dispone con acierto que la justificación de la excepción al derecho a consentir va más allá de la cualidad del sujeto que manipula los datos.

III.4.3. La excepción al consentimiento por determinación de la Ley.

Según el artículo 6.1 de la LOPD *"el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa"*. La Ley por lo tanto puede establecer excepciones a la necesidad de recabar el consentimiento del titular de los datos para que éstos puedan ser tratados. El contenido de este precepto se concreta en el RDLOPD[1749].

[1748] SÁNCHEZ CARO y SÁNCHEZ-CARO, *El Médico...,* cit., 2001, p. 137: "en segundo lugar, existe la necesidad de habilitar a las Administraciones Públicas en el correcto ejercicio de sus funciones y competencias. Dicha excepción se entiende, para que no haya lugar a dudas, a las instituciones y los centros sanitarios públicos y privados y a los profesionales correspondientes, que podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o haya de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad".

[1749] Artículo 10.2 RDLOPD: "*No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando: a) Lo autorice una norma con rango de ley o una norma comunitaria y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalzca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre. El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento un deber que le imponga una de dichas normas*".

La misma LOPD reconoce o subraya la aplicabilidad de esta excepción a los datos denominados sensibles entre los que están los relativos a la salud. En la regulación relativa a este tipo de información señala la norma que su tratamiento podrá realizarse bien con el consentimiento expreso del titular de los datos, o bien "*cuando por razones de interés general, así lo disponga una ley*"[1750]. En lo que se refiere a los datos relativos a la salud, por lo tanto, las normas con rango legal pueden considerar que de acuerdo a un interés general no es necesario dicho consentimiento. Sin duda alguna, el fundamento de esta regulación puede encontrarse en la Directiva europea de protección de datos sobre las categorías especiales de datos[1751].

En principio, parece justificable que el parlamento pueda fijar excepciones a la necesidad general de exigir el consentimiento, siempre que encuentre para ello argumentos suficientes fundamentados en la defensa de un interés digno de mayor protección. Así se ha reflejado en alguna resolución de la AEPD[1752].

A la hora de analizar esta excepción, la primera cuestión a dilucidar será la forma que deberá tomar la ley que fije la excepción al derecho a consentir[1753]. No parece haber dudas sobre el hecho de que se está ante una reserva de Ley[1754]. No obstante, ¿qué tipo de Ley ha de ser la que fije los límites al consentimiento? Esta cuestión ha sido tratada por la jurisprudencia precisamente al analizar la posible inconstitucionalidad de determinados preceptos de la LOPD. El TC afirma que los límites a los derechos fundamentales "pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE"[1755].

Este argumento hay que ponerlo en relación con preceptos ya conocidos de la CE, que disponen que el desarrollo de los derechos fundamentales y de las libertades públicas deberá

[1750] Artículo 7.3 LOPD.
[1751] Artículo 8.4 Directiva 95/46/CE: *"Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control"*.
[1752] Resolución AEPD, R/00645/2004, 26 de noviembre de 2004, procedimiento AAPP/00018/2004: "el legislador ha creado un sistema en que el derecho a la protección de datos de carácter personal cede en aquellos supuestos en que el propio legislador (constitucional u ordinario) haya considerado la existencia de motivos razonados y fundados que justifiquen la necesidad del tratamiento de los datos, incorporando dichos supuestos a normas de, al menos, el mismo rango que la que regula materia protegida".
[1753] OROZCO PARDO, "La Protección...", cit., 2002, p. 231: en relación al 6.1 LOPD que dice que una ley podrá limitar el consentimiento: "No se especifica el rango de esa ley, lo que permitiría establecer una grave limitación a un derecho fundamental por medio de una norma que no tenga el debido rango. En consecuencia, estimamos aplicable la doctrina expuesta acerca de la *reserva de ley* del art. 53.1 de la CE y la exigencia de los requisitos en ella establecidos."
[1754] APDCM, *Guía de Protección...,* Cit., 2004, p. 287.
[1755] STC de 30 de noviembre del 2000, FJ 11.

llevarse a cabo a través de una Ley orgánica[1756], y que sólo por Ley, se entiende que ordinaria, se regulará el ejercicio de los citados derechos y libertades[1757].

De estas consideraciones se desprende que la fijación de los límites, no de las formas de aplicar esos límites, deberá realizarse en todo caso a través de leyes orgánicas, lo cual obligará a exigir la mayoría absoluta del Congreso[1758] para la determinación de los mismos[1759]. Ciertamente, no es fácil en la práctica determinar dónde acaba el desarrollo y dónde comienza la ejecución[1760]. No obstante, no puede ponerse en duda que los límites de los derechos fundamentales constituyen un aspecto consustancial de los mismos y que por ello su fijación ha de llevarse a cabo a través de una Ley orgánica[1761]. Otra cosa será que una Ley ordinaria pueda entrar a concretar límites previamente fijados por una Ley orgánica.

La realidad es que en el ámbito sanitario diferentes normas con rango de Ley ordinaria establecen excepciones a derechos de los pacientes. En lo que concierne a la protección de datos, en los pocos casos en que una norma sectorial ha fijado límites a este derecho, se puede afirmar que se ha tratado de desarrollar lo que establece la LOPD, fundamentalmente en sus artículos 7 y 8[1762]. Como se verá, esta Ley orgánica establece una base lo suficientemente amplia, como para que el legislador ordinario tenga un extenso margen de actuación a la hora de limitar la facultad de consentir.

Otra de las cuestiones a aclarar respecto a la excepción al consentimiento que se analiza es la determinación de lo que se ha de entender por interés general. En lo que corresponde a los datos de salud, la facultad de autorizar la manipulación de este tipo de información se podrá limitar siempre que haya un interés general en juego. La utilización de este concepto de forma

[1756] Artículo 81.1 CE.
[1757] Artículo 53.1 CE.
[1758] Artículo 81.2 CE.
[1759] VALERO TORRIJOS y LÓPEZ PELLICER, "Algunas Consideraciones...", cit., 2001, p. 261, entienden que "cualquier excepción al núcleo esencial del derecho fundamental garantizado en el artículo 18.4,se realice mediante Ley Orgánica, de conformidad con la reserva contenida en el artículo 81.1 del mismo Texto Constitucional. En consecuencia, dado que no se trata de simples cuestiones conexas que justificarían una menor protección normativa, no parece admisible constitucionalmente la regulación con carácter de simple ley ordinaria de cuestiones tan relevantes como los supuestos en que puede prescindirse del consentimiento del afectado "; GUICHOT, *Datos Personales...,* cit., 2005, pp. 150-151.
[1760] DÍEZ PICAZO, *Sistema de Derechos...,* cit., 2005, p. 103; BRAGUE CAMAZANO, *Los Límites...,* cit*.,* 2004, pp. 322-323. STS 5 de febrero de 2008, FFJJ 4, 5, 6, 7 y voto particular, en relación al uso del conocido Sistema Integrado de Interceptación de Telefónica (SITEL).
[1761] SSTC, 13 de mayo de 1991, FJ 2 y 18 de julio de 1989, FJ 16.
[1762] Artículo 58.2 Ley 14/2007, 3 de julio, de Investigación Biomédica: "*El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización.*
No obstante lo anterior, de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable en el sentido del artículo 3.i. de esta Ley (...)"; Artículo 16.3, LBAP: "*El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (...). El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anominato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente (...)* ".

generalizada ha traído problemas de interpretación en la práctica jurídica, fundamentalmente cuando se ha empleado como límite a un derecho fundamental y cuando se ha erigido en criterio delimitador de las competencias del Estado y las Comunidades Autónomas. Parece claro que se refiere al interés de la colectividad, sin embargo, más allá de esta evidencia, el propio TC ha reconocido que el interés general constituye "un concepto abierto e indeterminado"[1763]. No obstante, y a pesar de concernir a una realidad difusa, hay que tratar de otorgarle un contenido concreto en la Ley de protección de datos.

Es criticable que en la determinación de excepciones a una facultad como la capacidad de autorizar o no el tratamiento de los datos de cada uno se empleen conceptos tan amplios como el citado, pues el margen de maniobra que se otorga al legislador es especialmente grande[1764]. La LOPD no llega a establecer un criterio a través del cual se pueda identificar el interés general en relación a esta excepción[1765].

En la Directiva europea sobre el tratamiento de los datos de carácter personal y en la Recomendación reguladora del tratamiento de los datos médicos se hace referencia a intereses de carácter general que prevalecen sobre el principio de calidad, el derecho de acceso, o el derecho a recibir información: a)la seguridad del Estado; b)la defensa; c)la seguridad pública; d)la prevención, la investigación , la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e)un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f)una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e)[1766].

La LOPD también establece excepciones similares, pero en relación a otras facultades distintas al consentimiento. Es el caso de las limitaciones impuestas al derecho a recibir información cuando los datos son tratados por la Administración: la defensa nacional, la seguridad pública o la persecución de infracciones penales se convierten en argumento suficiente para limitar el derecho a recibir información del titular de los datos.

Si bien las excepciones que se acaban de citar, tanto las de la Ley estatal como las de las normas de carácter supranacional, se refieren a facultades diferentes a la del consentimiento, es indudable que contienen el elemento de interés general que puede llevar a la limitación de las facultades más importantes que integran el derecho a la autodeterminación informativa. De esta forma, podrían comprenderse estos supuestos como ejemplo de lo que se puede interpretar como interés general a la hora de limitar el derecho a otorgar el consentimiento.

[1763] STC 11 de junio de 1984, FJ 4.
[1764] DE MIGUEL SÁNCHEZ, *Secreto Médico...,* cit., 2002, p. 283: "De constitucionalidad dudosa es también el art. 7.3 de la Ley al permitir que los datos sensibles (...) sean tratados recabados y cedidos sin consentimiento del interesado cuando así lo disponga la Ley por razones de *interés general*, residiendo (p. 284) nuevamente el problema en la escasa precisión de este concepto jurídico indeterminado".
[1765] MARTÍN CASALLO-LÓPEZ, "La Regulación...", cit., realiza la siguiente interpretación del artículo 7.3: las excepciones a las que alude el artículo 7.3 "son de naturaleza genérica o indeterminada, es decir, cualquiera que el legislador entienda como necesaria por responder a esa necesidad de interés general".
[1766] Artículo 13.1 Directiva 95/46/CE.

No se es muy partidario aquí de emplear la analogía como criterio a la hora de fijar excepciones a facultades tan relevantes como la que ahora se trata. La determinación de límites al derecho a consentir debería de realizarse mediante el empleo de disposiciones de mayor claridad. No obstante, ante la inseguridad que puede generar un concepto tan amplio como el de interés general, puede resultar práctico acudir a otras disposiciones, como las citadas, para averiguar la voluntad del legislador al emplear dicho término.

Partiendo de esta consideración, no se debe dar al concepto de interés general un sentido especialmente amplio. Se está hablando de limitar un derecho fundamental, por lo que el principio de proporcionalidad exige que la finalidad de la excepción sea de cierta envergadura. Puede afirmarse que en la mayoría de los casos este interés general estará vinculado a determinadas actividades de la Administración pública, y estará especialmente relacionado al concepto de interés público que en cierta medida se integra en el primero[1767]. No obstante, no toda actividad dirigida a la satisfacción de cualquier interés público puede llevar a la aplicación de la excepción que se plantea. Precisamente, atendiendo, como se ha hecho, a la normativa supranacional puede llegarse a la conclusión de que las finalidades de interés general que justificarán el tratamiento de los datos sanitarios sin el consentimiento del titular, cuando así lo disponga una Ley, serán las dirigidas a las que se han denominado en algún caso como "funciones públicas soberanas". Este concepto ha sido empleado por la jurisprudencia[1768] y hace referencia a "las funciones esenciales e irrenunciables del Estado", es decir aquéllas que "se orientan directamente a la satisfacción del bien común o interés general"[1769].

En lo que concierne a los datos relativos a la salud de las personas ya se ha visto al analizar el principio de finalidad que la salvaguarda de la salud abraza acciones concretas dirigidas precisamente a la promoción de ese bien común. Se hablaba entonces de investigaciones, estudios epidemiológicos, protección de la salud pública, etc. Las citadas acciones se dirigen a la protección de la salud colectiva. Parece indudable que fundamentándose en estos intereses una Ley puede limitar el derecho a emitir el consentimiento en lo relativo a los datos a salud. Sin embargo, más allá de estos supuestos que claramente se pueden identificar con el interés general, podría admitirse sin forzar la letra de la Ley que la salvaguarda de la salud individual constituye también un valor de interés común. La defensa de la salud de cada ciudadano constituye un fin de interés general. No hay que pasar por alto que esta finalidad se erige en elemento fundamental en la construcción de un sistema sanitario eficiente, objetivo que claramente trasciende el interés individual.

III.4.4. La excepción al consentimiento por motivos de salud: análisis de los artículos 7.6 y 8 de la LOPD.

Las excepciones que se acaban de comentar no responden a motivos estrictamente sanitarios. Es necesario centrar ahora la atención sobre los preceptos de la Ley que reconocen los límites con fundamento o base en causas sanitarias.

[1767] STS 22 de junio de 1999, FJ 2.
[1768] STS 13 de octubre de 1997, FJ 4.
[1769] VVAA, *Derecho Administrativo...,* cit., 1998, pp. 566-567.

III.4.4.A. La distinción entre los artículos 7.6 y 8 de la Ley.

En el articulado de la LOPD pueden reconocerse fundamentalmente dos preceptos que hacen referencia expresa al tratamiento de datos con finalidades sanitarias. El artículo 7.6 de la Ley regula el tratamiento de los datos especialmente protegidos con la finalidad de salvaguardar la salud de las personas. Por su parte, el artículo 8 se refiere exclusivamente al tratamiento de los datos de salud por parte de los profesionales en los centros sanitarios. De una primera lectura se podría concluir que la redacción de ambas disposiciones genera cierta confusión, pues en lo que toca a los datos relativos a la salud parecen recoger la misma regulación.

A) El primero de ellos señala que *"no obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.*

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento".

El contenido de este artículo no venía recogido en la Ley orgánica de protección de datos anterior. Este vacío generaba una situación de inseguridad entre los profesionales sanitarios que debían aplicar la norma, pues desconocían cuál era el régimen jurídico a seguir con respecto a los datos concernientes a sus pacientes[1770]. Hoy día la incorporación del precepto que ahora se comenta arroja cierta luz en el tratamiento de los datos de salud por el personal de los centros sanitarios. No obstante, su contenido plantea algunas dudas.

En primer lugar, se refiere a una lista de actividades que justifican el tratamiento de los datos denominados sensibles. La Ley alude a la "prevención", al "diagnóstico médico", a la "prestación de asistencia sanitaria", a "tratamientos médicos" y a la "gestión de servicios sanitarios". Fuera de estos casos no se podrán manipular los datos especialmente protegidos salvo que medie consentimiento del titular o habilitación legal[1771].

Esta regulación merece una doble crítica. Por un lado, plantea el eterno problema que persigue a toda norma que incorpora una lista. La taxatividad genera el riesgo de dejar alguna realidad fuera del ámbito de aplicación de esta disposición. Lo cierto es que en este caso, los conceptos que se utilizan son lo suficientemente amplios como para abrazar prácticamente toda la realidad sanitaria, por lo que parece difícil que este problema pueda darse.

[1770] CRIADO DEL RÍO y SEOANE PRADO, *Aspectos Médico-Legales...,* cit., 1999, pp. 142-143.
[1771] STC 8 de noviembre de 1999, FFJJ 3 y 4, en la que se niega la posibilidad de que en una entidad crediticia se empleen los datos de salud de los empleados con el fin de controlar el absentismo laboral.

Y por otro, sitúa al lector ante la necesidad de llenar de contenido cada concepto que incorpora: prevención, diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico y gestión de servicios sanitarios. No es fácil dar sentido propio a cada concepto empleado por este artículo pues la mayoría se refieren a realidades muy similares cuando no iguales. La distinción entre los ámbitos que abrazan el tratamiento médico y la asistencia sanitaria no parece que sea sencilla de llevar a cabo. El diagnóstico médico, por su parte, puede resultar integrado en los conceptos anteriores… Quizás hubiera sido más apropiado el empleo de un concepto más amplio, pero lo suficientemente concreto, dirigido a englobar todas las acciones que tienen por fin la salvaguarda de la salud de las personas.

En cualquier caso, parece clara la voluntad del legislador de abrazar en esta excepción todas las acciones dirigidas a proteger la salud de forma mediata o inmediata. La disposición comentada se refiere a la prevención, diagnóstico y asistencia, recogiendo todas las fases de la actuación sanitaria. Se trata, por lo tanto de un ámbito de realidad muy amplio.

En segundo lugar, se entiende que la inclusión del segundo párrafo no trae más que confusión. Este apartado se refiere al caso en que el tratamiento de unos datos de carácter personal es necesario para proteger el "interés vital" de un sujeto. Más allá de la indeterminación de esta expresión, ya puesta de manifiesto en la tramitación parlamentaria de la Ley[1772], cabe plantearse si este supuesto de hecho, el tratamiento de los datos sensibles para la salvaguarda del interés vital de los pacientes, no tiene cabida en el párrafo anterior del mismo artículo.

El concepto de interés vital puede entenderse en sentido estricto, referido sólo a las situaciones de vida o muerte[1773], o en un sentido más amplio, que abarca más supuestos que el citado[1774]. En cualquiera de los casos parece razonable comprender que la salvaguarda de un interés vital de una persona no es otra cosa que asistencia sanitaria. En la tramitación parlamentaria de la Ley ya se vincularon ambas realidades[1775], por lo que este segundo apartado, si bien fue incorporado por estar recogido en la Directiva europea, no origina más que confusión[1776]. Sería distinto si la regulación de la Ley fuera más concreta y estableciera criterios claros que determinaran cómo deben manipularse los datos en supuestos en que hay un interés vital en juego y en casos en que la asistencia sanitaria no deviene de situaciones de urgencia. No estableciendo directrices claras de regulación para las distintas situaciones, la redacción actual de la Ley genera incertidumbre.

Por último, es criticable también que este precepto no aclare si el consentimiento es necesario o no para llevar a cabo la manipulación de este tipo de datos para la realización de las citadas actividades[1777]. Como se verá, está hoy día asumida la interpretación de que de su letra se desprende un límite al derecho a la autodeterminación informativa, siempre que se justifique

[1772] HERRÁN ORTIZ, *El Derecho a la Intimidad...,* cit., 2002, p. 231.
[1773] COUDERT, "Tratamiento de datos ...", cit., 2007, p. 339.
[1774] ZABÍA DE LA MATA, "Supuestos que legitiman…", cit., 2008, p. 165.
[1775] HERRÁN ORTIZ, *El Derecho a la Intimidad...,* cit., 2002, p. 223:
[1776] TRONCOSO REIGADA, *Guía de Protección...,* cit., 2004, pp. 30-31.
[1777] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 131.

basándose en el fin de proteger la salud de las personas[1778]. La excepción parece deducirse, en términos algo confusos, del artículo 6.2 LOPD, que dispensa de la necesidad de recabar el consentimiento cuando la manipulación de datos tenga como fin proteger un interés vital en los términos del artículo 7.6[1779]. En cualquier caso, no se puede dejar de poner de manifiesto el hecho de que este límite no cumple con el requisito de previsibilidad exigible a toda excepción a un derecho fundamental.

B) Por su parte el articulo 8 de la Ley señala que "*Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad*".

Este precepto se refiere a la manipulación de datos relativos a la salud en los centros sanitarios por los profesionales que en ellos desempeñan su labor. La redacción de esta disposición tampoco es especialmente clara. Primero porque la remisión al artículo 11 de la Ley puede dar a entender que los demás preceptos de la misma no serán de aplicación a este tipo de tratamientos. Evidentemente, esta conclusión no es aceptable. El uso de los datos relativos a la salud necesariamente deberá cumplir las exigencias que derivan de principios tan importantes, recogidos en la LOPD, como el de finalidad.

Segundo, porque en este precepto no se recoge la posibilidad, como se hace en el anterior, de manipular los demás datos sensibles con la finalidad de proteger la salud de los ciudadanos. Si bien es cierto que no es común el uso de datos relativos a la ideología o creencias, o de carácter racial, con el fin citado, no se entiende porqué reconociéndose en ambos preceptos el mismo objetivo, en uno se autoriza su uso y no así en el otro.

Y por último, porque tampoco aquí se regula de manera clara si para este tipo de tratamiento es necesario el consentimiento del titular de los datos o no. El precepto parece realizar una remisión a la normativa sanitaria, pero no determina específicamente el régimen que habrá de seguir el uso de este tipo de información en este ámbito.

C) En cualquier caso, la principal confusión que generan los dos preceptos apuntados es la que deriva de la convivencia entre los mismos[1780]. De una primera lectura puede desprenderse que ambas regulaciones son muy cercanas. Merece la pena profundizar un poco más en este punto.

El artículo 7.3 se refiere al empleo, entre otros, de los datos relativos a la salud en general. En principio, para poder llevar a cabo un tratamiento de estos datos será preciso el consentimiento expreso del titular o la habilitación de una ley cuando haya un interés general en

[1778] Informe jurídico AEPD "Tratamiento de datos de salud", 2001.
[1779] Artículo 6.2 LOPD: "*No será preciso el consentimiento (...) cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6*". FERNÁNDEZ LÓPEZ, "Principio de consentimiento…", cit., 2010, p. 465, apunta también la confusión que deriva de la interpretación conjunta de los artículos 6.2 y 7.6 LOPD; DE MIGUEL SÁNCHEZ, "Datos de carácter personal…", cit., 2010, p. 712.
[1780] DAVARA RODRÍGUEZ, "Los Datos...", cit., 2000.

juego. Por su parte el artículo 7.6 de la LOPD se refiere al empleo de los datos sensibles, entre ellos los relativos a la salud, con fines sanitarios. Esta disposición hace referencia al uso de estos datos por los profesionales sanitarios, por lo que se imagina, en un inicio, que concierne a su manipulación en el ámbito estrictamente sanitario. El artículo 8 regula los supuestos en que los datos de salud son utilizados en el ámbito estrictamente sanitario. En este supuesto, al contrario de lo que ocurre en el precepto anterior, la referencia al uso de los datos en "las instituciones y los centros sanitarios públicos y privados" es expresa.

De los artículos 7.6 y 8 de la Ley se desprende que el contenido de ambos preceptos coincide plenamente en el ámbito al que se han de aplicar. Si se interpreta el primero de la manera en que se ha hecho más arriba carecería de sentido el segundo, que se refiere específica y claramente al tratamiento de los datos de salud en el ámbito sanitario y realiza, precisamente, una remisión normativa al ordenamiento sanitario, pues quedaría incluido en el contenido del 7.6.

Para salvar este problema interpretativo que plantea la LOPD, y otorgar un sentido propio a cada artículo, hay que entender que lo que se regula en el primero es el tratamiento de datos relativos a la salud por los profesionales situados fuera de los centros sanitarios, por ejemplo, en centros escolares, lugares de trabajo...[1781] La segunda disposición se referiría estrictamente al tratamiento de estos datos dentro del centro sanitario. En este sentido, el primero de los artículos parece tener un sentido más amplio que el segundo[1782].

En algún caso la doctrina ha entendido, partiendo de una interpretación literal de los preceptos, que estos artículos se distinguen por dos factores. En primer lugar porque, desde el punto de vista material, el artículo 8 abraza un ámbito de realidad más amplio que el otro. Según esta línea interpretativa el artículo 7.6 alcanzaría un espacio limitado prácticamente al tratamiento asistencial y a la gestión de los servicios sanitarios, mientras que en el otro se reconocería un concepto más amplio del derecho a la salvaguarda de la salud, donde tendrían cabida la investigación, la docencia, la realización de estadísticas, de inspección, etc[1783]. En segundo lugar, interpreta esta línea doctrinal que la Ley otorga un régimen diferente al tratamiento de los datos de salud en cada uno de estos artículos. Entiende que en el 7.6 se reconoce una excepción general al derecho a otorgar el consentimiento para el tratamiento, mientras que en el artículo 8 no se recoge tal limitación. En este precepto se reconocería simplemente una remisión legal a la normativa sanitaria que podría prever o no tal excepción al consentimiento.

[1781] Es claro que en ámbitos como el laboral, y sobre todo en sectores específicos en los que la salud de los trabajadores esté expuesta a mayores peligros, el control de la salud de los trabajadores es necesario. Así, la recogida y tratamiento de los datos sin el consentimiento del titular de los mismos en este ámbito está justificada debido a que la finalidad principal de estos tratamientos es la sanitaria. El Real Decreto 59/1997, de 17 de enero, por el que se aprueba el Reglamento de los Servicios de Prevención, en su artículo 37.3.d) dispone que "*el personal sanitario del servicio de prevención deberá conocer las enfermedades que se produzcan entre los trabajadores y las ausencias del trabajo por motivos de salud, a los solos efectos de poder identificar cualquier relación entre la causa de enfermedad o de ausencia y los riesgos para la salud que pueden presentarse en los lugares de trabajo*".

[1782] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182.

[1783] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182.

No se comparten aquí estas consideraciones. Más allá de lo que se vaya a comentar después sobre la regulación que se da al consentimiento en ambos artículos, la distinción que se realiza en relación al ámbito de aplicación de uno y otro artículo no se entiende acertada. El artículo 7.6 se refiere a aspectos muy variados en los que pueden tener cabida actuaciones como la investigación. En este sentido, al analizar el principio de finalidad se subrayó que la protección de la salud constituía un fin configurado por diferentes actuaciones. Entre éstas se situaba la acción preventiva, reconocida expresamente en el precepto señalado. No hay que forzar el sentido de dicho concepto para entender que la prevención de la salud abarca un extenso campo de actuación, donde indudablemente tienen cabida actividades como la investigación.

Dejando a un lado el criterio interpretativo que se acaba de señalar, se concluye que, en lo que toca a los datos relativos a la salud, tanto el artículo 7.6 como el 8 de la norma se refieren prácticamente a la misma realidad. Se trata de supuestos en que los profesionales sanitarios manipulan este tipo de datos con la finalidad de salvaguardar la salud de las personas. La única diferencia que da sentido a la convivencia entre ambos es que el primero se refiere al uso de la información fuera del ámbito sanitario y el segundo a su manipulación en los centros sanitarios.

III.4.4.B. El reconocimiento de la excepción al consentimiento en los artículos 7.6. y 8 de la LOPD.

Se ha criticado el hecho de que los preceptos que ahora se comentan no aclaren expresamente, si el tratamiento de datos relativos a la salud con fines sanitarios exige contar con el consentimiento del titular de los mismos. La LOPD es realmente confusa al respecto[1784].

Lo establecido por la Ley interna en el artículo 7.6 es una transcripción de lo dispuesto en la Directiva europea. Esta norma levanta, en primer lugar, la prohibición de manipular datos de salud cuando el empleo de la información resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto a la obligación de secreto u otra persona con semejante deber de secreto[1785]. En este apartado parece claro que la norma internacional exceptúa el requerimiento del consentimiento cuando los fines a perseguir son los citados. En segundo lugar, la prohibición queda anulada también cuando el empleo de dicha información se dirija a proteger el interés vital de una persona, siempre y cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento[1786]. Esta última referencia, que se recoge también en la LOPD, es menos clara

[1784] FERNÁNDEZ SALMERÓN, *La Protección de datos…,* cit., 2003, p. 287.

[1785] Artículo 8 Directiva 95/46/CE: "*1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.*
3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto".

[1786] Artículo 8 Directiva 95/46/CE: "*1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.*

que la anterior. De una lectura a *sensu contrario* se podría deducir, que cuando el paciente no está incapacitado deberá recabarse el consentimiento. Se cree aquí que este criterio no es correcto. Si se realiza una interpretación conjunta de todo el precepto la citada conclusión carece de sentido, pues no parece lógico que para la prevención o tratamiento médico se permita el tratamiento de datos de salud sin el consentimiento del titular y para proteger el interés vital de una persona, que resulta un bien jurídico merecedor de mayor protección, sea requerido cuando el sujeto esté en situación de darlo. Esta interpretación viene reforzada por la letra del ya citado artículo 6.2 LOPD.

El contenido de la Recomendación del Consejo de Europa es también similar. De su letra se desprende que los datos sanitarios pueden ser recogidos y procesados, siempre y cuando la Ley así lo permita, para fines médicos preventivos o para fines diagnósticos o terapéuticos relativos al afectado o a un pariente en línea genética[1787] o para salvaguardar intereses vitales del afectado o de una tercera persona[1788]. Señala, que los datos médicos pueden ser empleados también para fines de gestión del servicio médico, siempre que se hayan recabado con el objetivo de prevenir, diagnosticar o tratar terapéuticamente las enfermedades de los afectados[1789]. Se deduce de esta norma que mientras una Ley interna no disponga lo contrario la excepción al consentimiento para el tratamiento de datos con los citados fines tendrá aplicación.

De la normativa internacional se deduce que los fines dirigidos a proteger la salud de las personas legitiman la manipulación de datos. Tanto en la Directiva como en la Recomendación la finalidad de proteger la salud de las personas se recoge como un fin que legitima los tratamientos de datos, al igual que el consentimiento. Es decir, de la literalidad de su redacción se desprende que la legitimación de estas manipulaciones de datos, con fines sanitarios, es equivalente a la de un tratamiento de datos consentido por su titular. De esta manera no parece haber duda de que del contenido de estas normas resulta una excepción, de mayor o menor alcance, al consentimiento del titular. Siendo esto así resulta coherente pensar que este mismo régimen se sigue en el ámbito interno.

Como se ha dicho, el contenido de los señalados preceptos de la Directiva y la Recomendación se corresponde, en general, con lo que dicta el artículo 7.6 de la LOPD. Es fácil interpretar, por lo tanto, que en esta disposición de la Ley estatal se está reconociendo un límite al consentimiento. Así ha sido admitido por la doctrina[1790], y lo mismo parece haber hecho la jurisprudencia[1791]. Puede concluirse, por lo tanto, que el artículo 7.6 reconoce una excepción al derecho a otorgar el consentimiento[1792].

---

2. Lo dispuesto en el apartado 1 no se aplicará cuando: (...) c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento (...)"

[1787] Artículo 4.3.a).i, R (97) 5.

[1788] Artículo 4.3.a).ii, R (97)5.

[1789] Artículo 4.4 R (97) 5.

[1790] TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 31; NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182.

[1791] SAN 12 de abril de 2002, FJ 5.

[1792] STC de 8 de noviembre 1999, FJ 5.

La regulación que se acaba de exponer plantea un problema de interpretación. Se ha concluido que de la normativa internacional resulta sencillo deducir que en el artículo 7.6 LOPD se reconoce una excepción al consentimiento. Su alcance podrá ser discutible, pero no cabe duda de que se recoge un límite a la señalada facultad. Esta conclusión es fácil de extraer por cuanto las disposiciones de la normativa internacional y la estatal son muy similares. El problema deriva por el hecho de que, si bien la excepción al consentimiento del artículo 7.6 de la Ley encuentra fundamento en disposiciones de contenido similar del ordenamiento europeo, no ocurre lo mismo con el artículo 8 LOPD, que en este sentido se encuentra huérfano de referentes. En la medida en que esta disposición no aclara expresamente si recoge una excepción al consentimiento y que no cuenta con un precepto equiparable en el marco normativo internacional que ayude a aclarar su significado, resultará más complejo deducir el sentido de su contenido.

Hay que recordar que este precepto se refiere a la regulación del tratamiento de los datos en el ámbito sanitario, y realiza, con ese fin, una remisión a la normativa sanitaria, si bien salvando de dicha remisión al artículo 11 LOPD. Hay quien ha entendido que de esta regulación simplemente se deduce una remisión a la normativa sanitaria, teniendo que ser esta última la que determine si cabe limitar el derecho a la autodeterminación informativa o no[1793]. De esta manera, la LOPD, por sí misma, no fijaría la excepción al consentimiento informado para el tratamiento de datos de salud en el ámbito estrictamente sanitario con el fin de proteger la salud.

No se está de acuerdo con esta interpretación. Es cierto que la letra de la Ley, en el artículo 8, realiza una remisión a la normativa sanitaria, como también es cierto que hoy día la cobertura legal a la excepción se puede reconocer en el campo sanitario en diferentes normas como la LBAP de tanta cita[1794]. No obstante, se entiende aquí que interpretar este precepto como una mera remisión al legislador, que podrá o no exceptuar en este ámbito el derecho a consentir, es criticable.

Si este precepto se entendiera como mera remisión al legislador se estaría generando un vacío legal. Si lo único que previera la Ley fuera una remisión habría de estarse a lo que dijera la normativa sanitaria. Cierto es, como se acaba de apuntar, que hoy día la LBAP podría venir a cubrir esa laguna. Pero no es menos cierto que esta norma no determina con claridad la regulación del consentimiento para el tratamiento de datos sanitarios y que en los pocos preceptos en que se hace mención a esta cuestión plantea serias dudas que más adelante se pondrán de manifiesto. Además, siguiendo esa interpretación, debería entenderse que hasta que se ha aprobado la LBAP no ha habido una regulación específica sobre la materia. No parece razonable aceptar que la Ley dirigida a regular el tratamiento de datos de carácter personal pueda generar un vacío legal semejante en materia tan relevante como ésta. Piénsese en las consecuencias que esta situación podría acarrear para los profesionales sanitarios.

Resulta más acertado plantear una interpretación sistemática de la Ley, para extraer de su contenido cuál ha de ser el régimen jurídico a seguir con respecto al tratamiento de datos de

[1793] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182.
[1794] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 183.

salud en el ámbito estrictamente sanitario. Una interpretación sistemática de la LOPD lleva, sin necesidad de acudir a ninguna otra norma, a reconocer la excepción al consentimiento en el artículo 8.

A esta conclusión se llega interpretando que lo relevante a la hora de determinar el alcance de la excepción no es quién trate los datos, o dónde, sino la finalidad con que se empleen los mismos. Ya se ha subrayado anteriormente el carácter vertebrador del principio de finalidad. Es este criterio el que tiene que marcar la pauta a seguir en el tratamiento de datos. La interpretación contraria podría llevar a que una misma actividad, con un mismo fin, fuera tratada de diferente manera, en un caso exigiendo el consentimiento del titular y en otro no, por el mero hecho de que se lleve a cabo en un lugar u otro, fuera o dentro del ámbito sanitario. Teniendo en cuenta que el artículo 7.6 de la Ley reconoce la excepción al consentimiento para el tratamiento de datos de salud fuera del ámbito sanitario, parece lógico concluir que esta misma regulación se dará a la manipulación de estos datos, cuando se produce, precisamente, en su espacio natural, que no es otro que el del centro sanitario.

Esta interpretación ha parecido seguirse en alguna resolución de la AEPD[1795]. Encuentra apoyo también en el ámbito internacional. Hay que recordar que la normativa supranacional, a la hora de recoger la excepción que se plantea, no lleva a cabo distinción alguna entre datos de salud empleados dentro del ámbito sanitario y fuera de él. Las disposiciones que, tanto en la Recomendación del Consejo de Europa como en la Directiva europea, regulan el tratamiento de los datos de salud tienen un alcance general, sin realizar distinción alguna entre el ámbito sanitario y los demás sectores de la realidad. Simplemente disponen que para el cumplimiento de determinado fin el tratamiento de datos de salud podrá realizarse sin necesidad del consentimiento del titular. Una correcta trasposición de la Directiva europea parece que hubiera llevado a que la Lay estatal reconociera que tanto en el ámbito sanitario como fuera de él el límite al derecho que se analiza pueda ser aplicable.

Partiendo de lo que se ha dicho, se entiende que los dos preceptos de la Ley estatal que se analizan determinan los mismos criterios para el tratamiento de los datos de salud en diferentes ámbitos. En uno se regula la manipulación de estos datos fuera del ámbito sanitario y en el otro su uso dentro del mismo. No obstante, en ambos se establece la misma base jurídica. La manipulación de datos relativos a la salud se podrá llevar a cabo sin el consentimiento del titular siempre y cuando tenga por finalidad la protección de la salud de las personas. El desarrollo de este principio se llevará después a cabo en las diferentes normativas que regulen los distintos ámbitos de la realidad. En relación al artículo 8 será la normativa sanitaria la que se deberá tener en cuenta y la que concretará el régimen a seguir en el tratamiento de datos en este ámbito. En relación al artículo 7.6, serán otras normas las que lleven a cabo esa labor de concreción: la normativa laboral, etc.

Del contenido de las normas que se acaban de exponer se deduce una excepción al consentimiento. No parece haber duda sobre el hecho de que los fines que se señalan en las

[1795] Resolución R/00593/2009, de la AEPD, 25 de mayo de 2009, procedimiento nº PS/00638/2008, FJ 2.

disposiciones legitiman el tratamiento de datos sanitarios. El problema que plantean los señalados preceptos reside en determinar el alcance de dicho límite

III.4.4.C. El alcance de la excepción al consentimiento en el tratamiento de datos de salud en el ámbito sanitario.

III.4.4.C.a. La necesidad de aplicar un criterio flexible a la hora interpretar la excepción.

Se ha admitido que el artículo 8 LOPD reconoce un límite al consentimiento cuando se trata de manipular datos de salud en el ámbito sanitario. El alcance de esta excepción ha de determinarse poniendo en relación este precepto con las demás disposiciones de la misma Ley, fundamentalmente con el artículo 7.6, y la normativa sanitaria a la que se remite. El artículo 7.6 de la Ley, como ya se ha dicho, poniéndolo en relación con el artículo 6.2, parece abrir la puerta a una interpretación amplia de la excepción. Legitima el tratamiento de datos sensibles, entre los que están los de salud, cuando tiene como fin la prevención, el diagnóstico, la asistencia, la gestión de servicios sanitarios… Esta lista de finalidades abarca un amplio campo de actuación, por lo que podría justificar un sentido expansivo del límite al consentimiento. En relación a la normativa sanitaria, la LBAP parte de la posibilidad de que los profesionales tengan acceso a la historia clínica de los pacientes con fines asistenciales sin necesidad de requerir el consentimiento de éstos. No se limita esta alternativa a los casos de urgencia, sino que se expande por toda la actividad asistencial[1796]. Sin embargo, más allá de este ejercicio, fuera de la estrictamente asistencial, parece requerir el consentimiento. El tratamiento de datos sanitarios para realizar la actividad investigadora, de docencia, incluso la defensa de la salud pública, exige la autorización del titular[1797]. Se salvan de este requerimiento las actividades de gestión, administración, inspección y control de calidad, como ejercicios necesarios para poder llevar a cabo eficientemente la actividad asistencial[1798].

La interpretación del alcance de la excepción que propone el artículo 8 LOPD ha de partir de su relación con el artículo 7.6 de la misma Ley. La inevitable vinculación entre los dos preceptos que se estudian hace que para comprender el primero sea necesario atender al contenido del segundo.

[1796] Artículo 16.1 LBAP: "*La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia*".

[1797] Artículo 16.3 LBAP: "*El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos (…)*".

[1798] Artículo 16.4 LBAP: "*El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones*"; artículo 16.5 LBAPD: "*El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria*".

Antes de nada, hay que hacer referencia a un problema de relevancia que deriva de la letra del artículo 7.6. Este artículo determina un régimen jurídico que afecta al tratamiento de los datos de salud. Se refiere la disposición al "tratamiento", sin hacer mención alguna a la recogida o a la cesión. Por su parte, el artículo 8 sí regula la cesión pero no apunta nada en relación a la fase de recogida. Como se exponía en apartados precedentes, la falta de referencia en los citados preceptos a la fase de recogida podía conllevar el problema de no saber a qué operaciones les es aplicable el régimen jurídico contenido en las disposiciones. Se trataba de solventar esta confusión interpretando que el concepto de tratamiento se emplea aquí en un sentido amplio, y que la regulación recogida en dichos artículos es aplicable a todo tipo de operaciones. Esta interpretación encontraba base en la Directiva europea sobre protección de datos, que al regular la manipulación de los datos sanitarios utiliza únicamente el concepto de tratamiento, entendiéndolo en sentido amplio, y en la definición expansiva que la Ley estatal de protección de datos da de dicho concepto. Partiendo de esta consideración, si se interpreta que en los artículos 7.6 y 8 LOPD se reconoce una excepción al consentimiento, ésta será aplicable tanto a la recogida como al tratamiento. Esta idea, plantea un problema práctico, que tiene también sus consecuencias al interpretar las normas.

Hay que partir de que para manipular la información es necesario, primero, recogerla. En principio, si una persona consiente un tratamiento de datos se entenderá que consiente también su recogida, en la medida en que para manipular la información es necesario, primero, hacerse con ella. De la misma forma, si alguien remite los datos de forma voluntaria, se entiende inicialmente que consiente su manipulación. El problema surge cuando se ha de dar la vuelta a este planteamiento. ¿Cuando en las leyes se exceptúa el consentimiento para el tratamiento de datos, se está exceptuando también para su recogida? Si los datos se recaban de un tercero, caso de la cesión, no hay problema, pues la cesión se produce con un acceso del cesionario a los datos. Sin embargo, cuando la recogida se realiza tomando como fuente el propio titular de los datos, la excepción al consentimiento en la recogida se podría enfrentar a la negativa del titular a remitir la información. ¿Cómo se aplica la excepción en la práctica si el titular de los datos se niega a transmitir los datos? Este desajuste se produce debido a que la fase de recogida de datos del propio usuario plantea problemas específicos.

El principal problema reside en el hecho de que en el momento de recoger los datos pueden llegar a entrar en juego diferentes intereses y derechos más allá del derecho a la protección de la salud y la autodeterminación informativa que son los que aquí se estudian, así la integridad física, la intimidad corporal, la libertad, etc. Piénsese en todos los derechos que pueden verse afectados, por ejemplo, en una intervención corporal, que no deja de ser una operación a través de la cuál se recaban, también, datos. La LBAP dispone el deber de los pacientes de facilitar los datos sobre su estado físico y mental[1799]. Sin embargo, difícilmente puede entenderse de esta disposición una obligación a remitir datos[1800]. En principio parece difícil que se pueda obligar a

[1799] Artículo 2.5 LBAP: "*Los pacientes o usuarios tienen el deber de facilitar los datos sobre su estado físico o sobre su salud de manera leal y verdadera, así como el de colaborar en su obtención, especialmente cuando sean necesarios por razones de interés público o con motivo de la asistencia sanitaria*"

[1800] FERNÁNDEZ SALMERÓN, *La Protección de datos…,* cit., 2003, p. 286; MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 26

nadie a transmitir información sanitaria en contra de su voluntad con el fin de proteger su propia salud. Resulta esta conclusión, debido, precisamente, a que los intereses en juego hacen que prevalezca la autonomía del paciente sobre la posibilidad de obligar a alguien a que remita cierta información para asistirle médicamente. Evidentemente, esta circunstancia no quita para que el propio paciente tenga que soportar las consecuencias de no aportar la información solicitada, consecuencias que pueden afectar, incluso, a su salud[1801]. En este sentido, la aportación de los datos no sería otra cosa que una carga[1802].

Sea como sea, estas consideraciones, que serán objeto de un análisis más profundo en posteriores apartados, no han de desvirtuar la interpretación que se ha realizado más arriba de los artículos 7.6 y 8, al entender que reconocen una excepción al consentimiento. El que los datos deban ser entregados, la mayoría de las veces, voluntariamente, no quita para que los datos de salud puedan emplearse sin necesidad de la autorización de su titular, cuando se pretenden perseguir los fines fijados en los preceptos señalados[1803]. Otra cosa será que en esas operaciones entren en juego otros derechos e intereses que lleven a adoptar una solución diferente en situaciones concretas.

Realizado este apunte, lo que ahora hay que determinar es el alcance de la excepción al tratamiento de datos. Si bien en la Ley se parte de la necesidad del consentimiento expreso para el tratamiento de datos relativos a la salud de las personas[1804], posteriormente se rebaja esta protección cuando se emplea esta información con fines exclusivamente sanitarios[1805]. La justificación de esta excepción puede ser la siguiente: no es de ninguna manera viable ni razonable que los profesionales de la sanidad, cada vez que vayan a manipular datos de los usuarios con los fines citados, tengan que pedirles el consentimiento. Esta exigencia dificultaría gravemente la labor de dichos profesionales[1806], lo cual repercutiría en la calidad de la asistencia sanitaria en detrimento de la salud de los pacientes[1807]. Es indiscutible en estos casos que la vida de las personas y la salud constituyen bienes jurídicos más elevados que el derecho a la autodeterminación informativa[1808].

La excepción permite un tratamiento ágil de los datos cuando la finalidad es la protección de la salud de las personas. El alcance de este límite al derecho a consentir es muy genérico, por lo que a la hora de aplicarlo en la realidad cabe plantearse una serie de cuestiones. ¿Todas las

[1801] RODRÍGUEZ LÓPEZ, *La Autonomía…,* cit., 2004, p. 48; SAN JULIÁN PUIG, "Los principios generales…", cit., 2004, pp. 72-73; MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 26: "la falta de colaboración del paciente pudiera ser, si así resulta acreditado, una causa de exclusión de la responsabilidad del profesional".
[1802] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 276.
[1803] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 280, piénsese que la información sanitaria puede recabarse de investigaciones o de otras fuentes.
[1804] Artículo 7.3 LOPD.
[1805] Artículos, 7.6 y 8 LOPD.
[1806] SÁNCHEZ CARO y ABELLÁN, *Datos de Salud...*, cit., 2004, p. 58; MORALES PRATS, "Derecho a la Intimidad...", cit., 2001, p. 144; NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182: "En definitiva, de manera enrevesada y poco apropiada, se ha construido un sistema que finalmente beneficia al interés general que representa la agilidad en el ejercicio de la profesión médica, y que incide en la efectividad del derecho a la asistencia sanitaria, puesto que la exigencia de consentimiento expreso para tratar los datos cada vez que éstos se requieran en este ámbito es ciertamente muy poco operativa".
[1807] MORALES PRATS, "Derecho a la Intimidad...", cit., 2001, p. 142.
[1808] STC 11 de abril de 1985, FJ 3.

actividades que configuran la genérica finalidad de proteger la salud exceptúan de la misma manera este derecho? ¿Todo dato relativo a la salud merece el mismo tratamiento a la hora de aplicar la excepción? ¿El límite al derecho a consentir podría llevar en el ámbito sanitario a obligar a un sujeto a transmitir a los profesionales sanitarios información relativa a su salud? Desde una perspectiva práctica la aplicación del límite al consentimiento resulta una tarea sencilla.

En cuanto a las dos primeras interrogantes se puede partir de la siguiente consideración. Como se ha visto al analizar el contenido del artículo 7.6 de la Ley, la excepción abraza un ámbito especialmente amplio: prevención, diagnóstico, asistencia, actividades de gestión…[1809] Sin embargo, ya se ha dicho que las interpretaciones amplias a la hora de fijar límites a derechos fundamentales no tienen fácil encaje en el ordenamiento. Más aún cuando el límite no viene establecido de forma clara. Es necesario, por lo tanto, dar un sentido adecuado a la norma.

Desde un inicio han sido diferentes las interpretaciones que se han llevado a cabo de la disposición[1810]. Cierta jurisprudencia ha hecho un llamamiento a la necesidad de interpretar la excepción que se comenta de manera restringida[1811]. Dentro de esta forma estricta de leer el

[1809] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, pp. 92-93.

[1810] RUBÍ NAVARRETE, "Experiencias y criterios...", cit., 2006, p. 265: sobre el art. 7.6 LOPD: "En múltiples procedimientos sancionadores tramitados por la AEPD se han presentado alegaciones que tratan de amparar los más diversos tratamientos de datos de salud en este precepto. El elemento común a todas ellas conduce a considerar que la excepción contemplada en el artículo 7.6 tiene una naturaleza expansiva, que habilita cualquier tipo de tratamiento de datos de esta naturaleza. El criterio que subyace en esta alegaciones es el de que el artículo 7.6 no es una excepción a lo previsto en el artículo 7.3 de la misma norma, sino que es en regla general aplicable al tratamiento de este tipo de datos. Esta pretensión trata de apoyarse en la amplitud de situaciones que se recogen en dicho precepto, que abarcan desde el tratamiento de datos para la gestión de servicios sanitarios, a los más restringidos relacionados con el diagnóstico realizado por profesionales sanitarios.
Esta inversión de los criterios de aplicación de la LOPD ha sido sistemáticamente rechazada en las resoluciones de la AEPD y también por las sentencias de la Sala de lo Contencioso-Administrativo de la Audiencia Nacional"; CRIADO DEL RÍO, y SEOANE PRADO, *Aspectos Médico-Legales...,* cit., 1999, P. 141: hace una referencia la autora a diferentes posturas de diferentes autores con respecto a la necesidad de obtener el consentimiento informado para el tratamiento de los datos sanitarios: "GALÁN CORTES, J. C. (1999) expone que de acuerdo con la LORTAD se debe siempre informar y obtener el consentimiento del paciente antes de la informatización de los datos de la historia clínica.
HEREDERO, M. (1994) considera que no es necesario informar de los aspectos expuestos en el art. 5.1 de la LORTAD, en base al art. 5.3 (...) pero sí obtener el consentimiento previo a la informatización de los datos, porque no son aplicables las excepciones del consentimiento expuestas en la LORTAD. Otra cosa es en el ámbito de la Administración sanitaria, porque el art. 23 de la LGS habilita a las Administraciones sanitarias a que se creen registros y elaboren los análisis de información que sean necesarios para conocer las distintas situaciones de las que puedan derivarse acciones de intervención de la autoridad sanitaria. En base a este art. de la LGS este autor señala que el art. 8 de la LORTAD debe entenderse en el sentido de que las instituciones sanitarias están habilitadas para recoger y tratar automáticamente los datos de salud, y que en este caso entraría en juego la excepción del consentimiento del art. 6.2 de la LORTAD <<cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias>>.
SÁNCHEZ CARO, J. (1999), en base a las excepciones al consentimiento que expone la propia LORTAD, interpreta que cuando el paciente acude voluntariamente a un centro sanitario su información se puede automatizar porque lo permite la ley, lo cual no significa que no deba ser informado de que sus datos se van automatizar. (p. 142) En sentido contrario, CASTELLS ARTECHE, J. M. (1997) opina que no es necesaria la información del afectado antes de proceder a la informatización de sus datos, sobre todo en el caso del médico en el ejercicio privado, pero sí que es necesario el consentimiento del afectado previo al tratamiento automatizado de los datos de carácter personal".

[1811] SSAN, 31 de mayo de 2002, FJ 4; 26 septiembre 2002, FJ. 3: "es la regla general la exigencia del consentimiento inequívoco del afectado para el tratamiento de datos de carácter personal (...) y sabemos que el legislador ha querido reforzar esta exigencia cuando se trata de datos especialmente protegidos (...), las excepciones a dicha norma general,

límite se han dado diferentes interpretaciones. Alguna resolución de la AEPD ha apuntado que la excepción al consentimiento sólo será aplicable a los casos en que una disposición así lo establezca o sea estrictamente necesario para salvaguardar la salud de los usuarios atendiendo a las circunstancias de cada caso[1812]. Hay quien ha entendido que el límite al derecho a consentir sólo podrá aplicarse en casos de urgencia[1813]. Esta interpretación podría encontrar apoyo en una lectura literal del artículo 7.6 en relación al 6.2 de la LOPD. Este último precepto expresamente recoge una excepción al consentimiento remitiéndose al artículo 7.6, pero haciendo referencia, únicamente, a los supuestos en que está en juego un interés vital. De esta redacción resultaría fácil deducir que sólo en los casos de cierta urgencia puede exceptuarse el consentimiento.

También se ha admitido, desde una perspectiva más laxa, que el límite se aplica a los actos vinculados directamente con la asistencia sanitaria, más allá de los casos especialmente graves, pero no a la realización de otros fines dirigidos también a proteger la salud, como las investigaciones, actividad docente, etc[1814]. Esta última forma de interpretar la excepción podría encontrar apoyo en la LBAP. Como se ha visto, esta norma parte de la posibilidad de manipular datos sanitarios sin necesidad de la autorización del titular de los datos cuando la finalidad es asistencial[1815]. Fuera de la actividad estrictamente asistencial parece exigir el consentimiento[1816], si bien salvando de este requerimiento las funciones de gestión, administración, inspección y control de calidad, al ser ejercicios necesarios para poder llevar a cabo eficientemente la actividad asistencial[1817]. Más allá de esta Ley, en el ámbito sanitario son diferentes las normas que afectan puntualmente al tratamiento de datos de salud, como en relación a los estudios epidemiológicos, a la farmacovigilancia, etc. En muchas ocasiones, como se apreciará en el apartado dedicado a estudiar la cesión de datos, estas normas constituyen base suficiente para manipular información sanitaria sin necesidad del consentimiento de sus titulares. Sin embargo, dejando a un lado estas referencias concretas, lo cierto es que la LBAP da pie para interpretar la excepción al consentimiento en sentido relativamente estricto. También se sigue esta forma de entender la excepción en otros textos de carácter internacional[1818].

---

como la prevista en el artículo 7.6, deben ser interpretadas de modo estricto sin que queda admitir otros casos de dispensa del consentimiento distintos al que aparece expresamente contemplado en la norma".

[1812] Informe jurídico AEPD, 2001, sobre Tratamiento de Datos de Salud: "estas dos últimas especialidades al régimen general, tanto la del artículo 8 como la del 7.6 no pueden interpretarse de forma genérica o extensiva (...) sino que debe restringirse a los dos supuestos en que únicamente serán de aplicación, esto es: que una disposición normativa establezca y disponga con carácter específico un tratamiento de tales datos, o bien que el mismo resulte efectivamente necesario e imprescindible, y ello se justifique debidamente en cada caso. Fuera de estos dos supuestos excepcionales, el régimen aplicable con carácter general es el del artículo 7.3 de la LOPD". MARTÍ MONTESINOS y PIDEVALL BORRELL, "Accesos a la Historia Clínica...", cit., 2004, Pp. 107-108.

[1813] GUERRERO PICÓ, *El Impacto...,* cit., 2006, p. 265: en relación al 7.6 LOPD: "Por la remisión que hace al art. 7.6 LOPD, que permite el tratamiento sin consentimiento de datos sensibles cuando así lo justifiquen razones de urgencia médica, el interés del que habla la LOPD ha de referirse únicamente a la salud del interesado y deberá interpretarse muy restrictivamente, siendo necesario apreciar una verdadera urgencia, algo que resulta dudoso en lo que respecta a la gestión de servicios sanitarios a la que alude igualmente el art. 7.6 LOPD".

[1814] NICOLÁS JIMÉNEZ, *La Protección...,* cit., 2006, p. 182; MURILLO DE LA CUEVA, "El Derecho...", cit., 2006, p. 40-41; LÓPEZ ULLA, "El consentimiento del afectado…", cit., 2010, p. 681.

[1815] Artículo 16.1 LBAP.

[1816] Artículo 16.3 LBAP.

[1817] Artículo 16.4 LBAP y artículo 16.5 LBAP.

[1818] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.

Desde otra perspectiva, se ha entendido que las disposiciones de la LOPD que se comentan pueden tener un ámbito de aplicación más amplio. La excepción al consentimiento en el tratamiento no se puede limitar a los casos de urgencia, ni siquiera a la actividad asistencial, sino que ha de tener una mayor expansión[1819]. De lo que ha dispuesto algún informe jurídico de la AEPD se podría desprender que el ámbito que abarca el artículo 7.6 de la Ley no se limita a operaciones concretas, sino que abraza todas las actividades que en la normativa sanitaria se entienden necesarias para salvaguardar la salud de las personas[1820]. En este caso, la remisión del artículo 6.2 LOPD, que reconoce una excepción al consentimiento, al 7.6 no se limitaría a los supuestos de urgencia, sino a todas las actividades que se citan en esta última disposición. En algún momento la jurisprudencia también ha parecido dar una interpretación amplia al contenido de la excepción, englobando actuaciones de diverso tipo, entre las que tienen cabida también las operaciones que no son asistenciales[1821]. En la práctica, en algún caso se ha aplicado sin ambages esta interpretación amplia. Es el caso del Servicio Vasco de Salud-Osakidetza que llevó a cabo un cambio de estructura del sistema que soportaba la información sanitaria, centralizando las bases de datos. En este supuesto, el traslado de los datos sanitarios de todos los usuarios a una única base de datos se consideró como una operación dirigida a la salvaguarda de la salud, con lo que no era preciso el consentimiento de sus titulares[1822]. La doctrina también parece haberse decantado en algún momento por comprender que la salvaguarda de la salud de las personas, con todas las operaciones que integra, reclama en todo caso la excepción al consentimiento[1823].

Esta interpretación si bien facilitaría mucho la comprensión de la letra de la Ley en este punto, supondría olvidar que el enfrentamiento entre diferentes bienes jurídicos ha de salvarse con la búsqueda de un equilibrio justo entre los mismos. Una interpretación tan amplia como la expresada llegaría a vaciar de contenido, de manera innecesaria, la autodeterminación informativa a favor del derecho a la protección de la salud. No parece que todas las operaciones dirigidas a la protección de la salud hayan de ser comprendidas de la misma forma. La excepción al consentimiento no alcanza de igual manera a todas las actuaciones dirigidas al cumplimiento de la citada finalidad.

[1819] MÉJICA y DÍEZ, *El Estatuto...,* cit., 2006, pp. 71 y siguientes.

[1820] Informe jurídico 005/2006, AEPD, donde dice que "La Agencia Española de Protección de Datos ha venido considerando que los supuestos englobados bajo la habilitación del artículo 7.6 de la Ley Orgánica ha de entenderse relacionado con la cobertura y asistencia sanitaria regulada por la legislación estatal y autonómica en materia de sanidad". Como se ha visto más arriba, tanto la legislación estatal como la autonómica reconocen dentro de esa actividad actuaciones estrictamente asistenciales y otras que tienen que ver con la investigación o estudios epidemiológicos.

[1821] SAN, 23 noviembre 2006, FJ. 3: "La prestación del servicio médico realizado por los facultativos de la mercantil recurrente, no tiene por objeto ni la mejora, ni la prevención de la salud de las personas a quienes examina y cuyos datos incorpora al fichero, es decir, no realiza una prestación necesaria para su salud, ni tampoco para el tratamiento médico a que pudieran estar sometidos, ni para la investigación científica o el desarrollo de la medicina, sino que la prestación únicamente están al servicio de los intereses del arrendador que, a través de ese mecanismo, pretende evitar el absentismo en el trabajo". Parece que en esta resolución se da a entender que cuando la finalidad es la investigación científica la necesidad de consentimiento aparece exceptuada.

[1822] Comparecencia del Consejero de Sanidad INCLAN IRIBAR, Gabriel ante la Comisión de Sanidad del Parlamento Vasco, para informar sobre el proyecto Osabide. Diario de Comisiones del Parlamento Vasco, 23 de mayo de 2002.

[1823] HEREDERO HIGUERAS, "La Protección...", cit., 1994, p. 21.

Ciertamente, no resulta sencillo tratar de dar una interpretación definitiva de los preceptos que se analizan[1824]. Si bien partiendo de la LBAP podría asumirse un criterio restrictivo, la LOPD puede suponer la base para una interpretación más amplia. Se aboga aquí por dar un criterio más flexible al propuesto por ambas corrientes. Se interpreta que la excepción al consentimiento se aplicará más allá de que la finalidad de una actuación sea asistencial, de investigación, o de otra índole. Su aplicación dependerá, sobre todo, de la realización de un juicio de proporcionalidad previo que determine en cada caso si es posible limitar el consentimiento. Este criterio puede encontrar su fundamento jurídico en el propio ordenamiento. Primero, porque los diferentes criterios que parecen emplear las distintas normas llevan a tener que abogar por una interpretación conjunta de todo el ordenamiento. Y segundo, porque tanto la Ley estatal[1825], como la Directiva europea[1826], disponen que el tratamiento de los datos de salud se realizará en caso de que sea "necesario" para conseguir los fines que se han comentado. No es difícil interpretar este criterio de necesidad como un llamamiento a la aplicación del principio de proporcionalidad: la excepción se aplicará cuando sea necesario.

III.4.4.C.b. Determinación de los supuestos exceptuados de la exigencia de recabar el consentimiento.

Se tratará en este momento de realizar un acercamiento a los supuestos en que la excepción al derecho a consentir el tratamiento de datos de salud alegando motivos sanitarios es posible. Se dice que se hará un acercamiento, debido a que es una cuestión sobre la que se profundizará al tratar la cesión de datos. Esto es así porque gran parte de las operaciones que se llevan a cabo en el ámbito sanitario en relación a los datos de carácter personal son transmisiones de datos.

Los límites que se van a citar ahora afectan al consentimiento vinculado al tratamiento de datos, no a la cesión. Se realiza esta distinción porque el régimen jurídico que se aplica a las cesiones es diferente. Muchas de las manipulaciones que se producen en el ámbito sanitario son transmisiones de datos entre profesionales sanitarios, o estos y otros sujetos extraños a la práctica sanitaria, que los emplearán con los más variados objetivos. Pues bien, no se está haciendo referencia ahora a estos supuestos, sino a los casos en que los datos han sido directamente recogidos del propio paciente para ser empleados con un objetivo determinado.

En la práctica este tratamiento se produce cuando el usuario se presenta ante los profesionales sanitarios, sea personal médico o administrativo, y transmite la información pertinente, para que sea manipulada directamente por diferentes sujetos, con distintos fines. Los motivos principales que llevarán a los ciudadanos a dar información sobre su persona a los profesionales sanitarios serán los asistenciales y administrativos. Piénsese en el caso común en que una persona acude a su médico de cabecera a recibir un tratamiento médico o cuando alguien transmite datos identificativos en un centro con fines administrativos como la creación de la Tarjeta Sanitaria. Más allá de estos supuestos podría imaginarse el caso en que se transmiten

[1824] SÁNCHEZ CARO y ABELLÁN, *Datos de...,* cit., 2004, p. 33.
[1825] Artículo 7.6 LOPD.
[1826] Artículo 8.3 Directiva 95/46/CE.

datos con el fin de realizar una investigación, como en los ensayos clínicos. En estas situaciones los pacientes o usuarios remiten la información a los profesionales pertinentes y estos directamente manipulan los datos para cumplir sus funciones. Lo que ahora interesa es analizar hasta qué punto la información contenida en las historias clínicas y demás ficheros puede ser empleada por los profesionales sanitarios sin su autorización. La solución a esta cuestión ha de darse atendiendo a la finalidad que se persigue con la manipulación de datos y al principio de proporcionalidad.

En primer lugar, habrá que entender exceptuado el derecho a otorgar el consentimiento cuando el derecho a la información ha sido limitado. Esta consideración, como ya se dijera en su momento, tiene pleno sentido, pues el consentimiento para ser válido deberá ser informado. Así, si el deber de informar se encuentra exceptuado será difícil que el consentimiento informado pueda emitirse[1827]. En todo caso, hay que recordar que en la práctica las limitaciones al mismo en el ámbito sanitario no son excesivas, habida cuenta del sistema propuesto.

En segundo lugar hay que plantearse cuándo se puede limitar el derecho a consentir una manipulación de datos por motivos estrictamente vinculados a la protección de la salud.

A) Primero, no parece haber problema en afirmar que en situaciones de urgencia no será necesario recabarse la autorización del afectado o interesado. Cuando un sujeto se encuentra en esta circunstancia pueden darse diferentes supuestos. Puede estar inconsciente y sin una persona que ejerza como su representante. En este caso los argumentos para justificar la excepción al consentimiento son claros. Por un lado la Ley así lo reconoce de manera clara[1828]. Por otro, hay que tener en cuenta que la salud se encuentra afectada de manera grave y que la rapidez de actuación suele ser indispensable. Parece razonable pensar que el derecho a la autodeterminación informativa ha de ceder a favor del derecho a la protección de la salud.

El sujeto también puede estar consciente o encontrarse con un sujeto habilitado para dar el consentimiento en su nombre. La LOPD señala que pueden manipularse datos sensibles con el fin de proteger un interés vital cuando el afectado está física o jurídicamente incapacitado. De la letra de la Ley podría interpretarse que cuando el sujeto es capaz para emitirlo deberá solicitarse su consentimiento. Esta regulación parece recoger la misma fórmula que se emplea en la normativa sanitaria para regular el consentimiento informado dirigido a autorizar tratamientos médicos. Según la LBAP los profesionales sanitarios pueden llevar a cabo intervenciones clínicas indispensables para proteger la salud de un paciente, sin necesidad de recabar su consentimiento, cuando se dé una situación de urgencia y el afectado no esté capacitado para otorgar su autorización[1829]. Se desprende de esta redacción que cuando el afectado esté capacitado será necesario su consentimiento, incluso en estos casos de urgencia. Se refuerza con esta regulación el principio de autonomía, dejando a las personas un mayor margen de decisión.

[1827] SÁNCHEZ CARAZO, *La intimidad...*, cit., 2000, p. 139.
[1828] Artículo 6.2 y artículo 7.6 LOPD.
[1829] Artículo 9.2.b) LBAP.

Teniendo en cuenta la similitud del contenido de las normas dirigidas a regular la protección de datos y la normativa sanitaria se podría dar por buena la interpretación que lleva a concluir, que en casos de urgencia médica es necesario el consentimiento del titular de los datos para manipular la información con fines asistenciales, cuándo haya posibilidad de recabarlo. No parece que esta forma de entender el precepto tenga justificación. Cuando en la normativa sanitaria se refuerza el principio de autonomía a favor de los pacientes en los supuestos en que éstos van a ser sometidos a una intervención clínica, se hace teniendo en cuenta factores que no se dan en el ámbito de la protección de datos. En el campo estrictamente asistencial la apuesta por otorgar un mayor espacio de actuación a la voluntad de los pacientes se produce porque las actividades clínicas en circunstancias de urgencia, y también en las que no son de urgencia, se sitúan en parámetros muy concretos. En estas situaciones el paciente ha de valorar los riesgos y las ventajas de las alternativas médicas propuestas por los profesionales y adoptar una decisión, en la que se pueden ver involucrados derechos como la vida, la integridad física y moral, etc. La exigencia del consentimiento se dirige a reforzar la posición de cada persona, que decidirá qué hacer con su salud. Cuando lo que ha de consentir el paciente es la manipulación de unos datos no entran en juego estos parámetros. En este supuesto colisionarán de forma inmediata el derecho a la autodeterminación informativa y el derecho a la protección de la salud de las personas.

Afectados simplemente los derechos a la autodeterminación informativa y a la protección de la salud, en una situación de urgencia los profesionales sanitarios han de tener vía libre para acceder a la historia clínica del paciente, incluso frente a la oposición del mismo[1830]. Esta conclusión encuentra a su favor un argumento de relevancia práctica, que tiene aplicación en todos los casos en que los datos se emplean con fines asistenciales. Hay que tener en cuenta que si no se permite el acceso y manipulación de datos a los profesionales, éstos no podrán determinar el alcance de la urgencia, ni el tratamiento necesario a aplicar, ni las alternativas. La manipulación de datos constituye un *prius* necesario para llegar a un estadio en que la actividad sanitaria pueda desarrollarse con plenitud. Sin ánimo de restar valor al derecho a la autodeterminación informativa, no hay que olvidar que la manipulación de datos constituye un medio para proteger la salud de las personas. Sin la información no se puede alcanzar la situación en que, por ejemplo, es posible emitir un diagnóstico determinado y concretar las diferentes opciones de tratamiento. Se entiende aquí que la posibilidad de alcanzar esta situación bien justifica la posibilidad de exceptuar el consentimiento del titular en los supuestos a los que ahora se hace referencia. Otra cosa será la oposición que pueda interponer el paciente, una vez se haya manipulado la información pertinente que ayude a extraer las conclusiones necesarias, a un tratamiento médico determinado.

B) Segundo, cabe plantearse si en el ejercicio de la asistencia sanitaria, que no sea en situaciones de urgencia, cabe aplicar la excepción al consentimiento o no. El análisis se antoja más complejo que el arriba citado, en la medida en que las circunstancias hacen que los bienes jurídicos en juego tengan relevancia jurídica similar. Sin embargo, y como se analizará en el apartado dedicado a la cesión de datos, la normativa aporta argumentos suficientes para apoyar

[1830] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, p. 32.

la primacía de la salud sobre el derecho a otorgar el consentimiento. Por poner un ejemplo, la normativa sanitaria exige que los profesionales sanitarios tengan acceso a las historias clínicas en el ejercicio de su labor asistencial[1831]. Es más, y aunque pueda parecer una situación controvertida, de la redacción de las citadas normas podría llegar a concluirse que la manipulación puede darse incluso en caso de oposición del usuario o paciente.

En estos supuestos en que el titular de los datos se opone expresamente a su tratamiento no se encuentra una normativa específica que aclare cuál ha de ser la forma de actuar. En principio, si el usuario transmite la información voluntariamente parece que a su vez autoriza su tratamiento. Sin embargo, cabe preguntarse qué sucedería si posteriormente se negara a que la información se manipulara con fines sanitarios. Lo mismo podría ocurrir en el caso en que la información se recabara en un momento en que el paciente se encontrara en estado de inconsciencia y posteriormente se opusiera a que dichos datos fueran empleados para proteger su salud. ¿Se impondría el derecho a la autodeterminación informativa o el derecho a la protección de la salud?

Las normas sanitarias podrían servir de base para interpretar que la oposición del titular de los datos es superable, a favor del tratamiento de los datos. También podrían serlo las normas de protección de datos, que habilitan la manipulación de datos de salud con fines asistenciales, sin fijar límite alguno a dicha posibilidad de tratamiento. Sin embargo, como ya se comentara, estas previsiones normativas son especialmente genéricas, por lo que plantean la duda de su alcance. Frente a estos argumentos el principio de autonomía podría justificar también la validez de la oposición frente a la necesidad de manipular información. El principio de autonomía podría llevar a justificar que el titular de los datos, que es a su vez el titular del derecho a la protección de la salud que está en juego, impusiera su voluntad.

Quizás la solución más adecuada vendría de realizar un juicio de proporcionalidad en cada supuesto en que se diera la oposición, atendiendo a cómo afectaría a la protección de la salud el cumplir con dicha oposición y a la forma en que, en caso de no respetar la voluntad del titular, la manipulación de determinados datos de salud vulneraría la intimidad y la autodeterminación informativa del paciente.

En principio, el afectado podría oponerse a la manipulación de determinados datos que constaran en la historia clínica y que considerara afectan de manera grave a su intimidad. El principio de autonomía y la protección de la intimidad y la autodeterminación informativa se situarían en una posición más elevada que la protección de la salud. Sin embargo, como se acaba de señalar más arriba, hay que tener en cuenta que, en la práctica, para concluir si una situación es grave hay que acceder a determinada información del paciente. Atendiendo a esta circunstancia se entiende que cuando hubiera indicios de cierto riesgo para la salud se debería

[1831] Artículo 16.1 LBAP; Artículo 11.2, Ley 21/2000, de Cataluña, 29 de diciembre del 2000, sobre los Derechos de Información relativos a la Salud, la Autonomía del Paciente y la Documentación Clínica: "*La historia clínica es un instrumento destinado fundamentalmente a ayudar a garantizar una asistencia adecuada al paciente. Con este fin, los profesionales asistenciales del centro que están implicados en el diagnóstico o el tratamiento del enfermo han de tener acceso a la historia clínica*".

estimar la facultad del profesional para acceder a la historia clínica, salvando la oposición del paciente.

De aquí se concluye que cuando la manipulación de los datos tiene como objetivo tratar a una persona médicamente, el empleo de los datos de salud no requerirá de la autorización de sus titulares. Cuando se trata de cumplir con fines asistenciales, los profesionales podrán acceder a los ficheros en que constan los datos recabados del propio titular para manipular esa información.

C) Tercero, en el supuesto de que la actuación no se dirija a la asistencia sanitaria directa las circunstancias que rodean al caso serán otras. Cabe plantearse, por ejemplo, si es posible aplicar la excepción cuando el objetivo de la manipulación de datos es la investigación. En relación al tratamiento de datos de salud con fines de investigación, lo que aquí interesaría sería ver es si es posible exceptuar el consentimiento de un sujeto para manipular información que ya ha sido recabada, con dichos objetivos. Se trata del supuesto en que diferentes agentes acceden a información ya obrante en distintos ficheros de los sistemas sanitarios, caso de las historias clínicas, con el fin de llevar a cabo investigaciones. Piénsese en el caso en que un equipo de investigadores de un centro accede a diferentes historias de personas que tienen una misma enfermedad, con el fin de analizar la evolución y características de dicha patología. Esta manipulación posterior, vinculada a la investigación, se refiere a una remisión a otro órgano de datos obtenidos durante una anterior asistencia o una investigación realizada previamente sobre el cuerpo de un paciente. Se puede observar que la posibilidad de llevar a cabo estas operaciones hace referencia a transferencias de datos entre diferentes agentes, con lo que esta cuestión será analizada en el apartado dedicado a la cesión. Se pueden adelantar, sin embargo, unas conclusiones. Estas operaciones requerirán, la mayoría de las veces, del consentimiento del titular, o de una previa disociación de los datos[1832].

La finalidad investigadora puede llevarse a cabo también mediante operaciones desarrolladas directamente sobre el propio paciente. Se está haciendo referencia a la posibilidad de recoger los datos del propio paciente con fines de investigación. Esta circunstancia se produce, la gran mayoría de veces, mediante operaciones sobre el propio cuerpo del paciente. Cabe plantearse si en estas operaciones es posible recabar información sobre la salud de los implicados sin su consentimiento. Esta cuestión se analizará en el apartado siguiente, sin embargo, pueden adelantarse algunas apreciaciones.

La CE reconoce la libertad de investigación[1833] y reclama de los poderes públicos la promoción de la ciencia y la investigación científica[1834]. Sin embargo, la propia norma dispone como límite a esta actividad la intimidad de las personas[1835]. En la línea de esta regulación, y

[1832] SÁNCHEZ CARAZO, *La intimidad…,* cit., 2000, p. 205.
[1833] Artículo 20.1 CE: "*Se reconocen y protegen los derechos: b) A la producción y creación literaria, artística, científica y técnica*".
[1834] Artículo 44.2 CE: "*Los poderes públicos promoverán la ciencia y la investigación científica y técnica en beneficio del interés general*".
[1835] Artículo 20.4 CE: "*Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las Leyes que lo desarrollan y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a al protección de la juventud y de la infancia*"

centrándose en el ámbito sanitario, la LBAP señala que es necesario el consentimiento del titular para manipular los datos de salud con fines de investigación, cuando éstos no puedan disociarse[1836]. Esta consideración, en la que prevalece el derecho a la protección de datos, resulta también de la normativa sobre ensayos clínicos y la investigación biomédica[1837].

Cuando la investigación se da directamente sobre el cuerpo del paciente, caso de los ensayos clínicos o la investigación biomédica, el paciente o usuario participa en la operación. En la medida en que la participación de las personas en dichas investigaciones se sujeta a la voluntad de los propios ciudadanos, la recogida de los datos y su manipulación dependen también de esta autorización. No se pueden recabar datos del paciente sin intervenir en su cuerpo o sin que éste transmita los datos, y esta intervención no se puede realizar sin su consentimiento, por lo tanto la conclusión es sencilla: si se ha de consentir la operación, la recogida de los datos y su tratamiento ha de ser autorizada. En estos casos la aplicabilidad del límite al consentimiento se reduce a supuestos muy concretos en que las intervenciones pueden desarrollarse sin autorización del titular. Esta circunstancia podría tener cabida en las normas. Pueden reconocerse determinadas situaciones en que es posible que el sujeto sea sometido a esas operaciones sin necesidad de recabar su autorización[1838].

[1836] Artículo 16.3 LBAP. En el mismo sentido el artículo 5 Convenio para la protección de los Derechos Humanos y la Dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina, aprobado por el Comité de Ministros del Consejo de Europa, Oviedo 19 de noviembre de 1996: "*Una intervención en el ámbito de la sanidad sólo podrá efectuarse después de que la persona afectada haya dado su libre e inequívoco consentimiento* (…)".

[1837] Artículo 60.4 Ley 29/2006, 26 de julio de 2006, de Garantías y Uso Racional de Medicamentos y Productos sanitarios; artículo 3.6 RD 223/2004, 6 de febrero, por el que se regulan los Ensayos Clínicos con Medicamentos. Artículo 4 Ley 14/2007, 3 de julio de 2007, Investigación Biomédica. SÁNCHEZ CARAZO, *La intimidad…*,cit., 2000, p. 205; BORDES SOLANAS, "Investigación médica…", cit., 2006, p. 230; SÁNCHEZ CARO, "La Protección de Datos…"*,* cit., 2009, p. 87.

[1838] Artículo 60 Ley 29/2006, de 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios: "*4. El sujeto del ensayo prestará su consentimiento libremente, expresado por escrito (...). 5. Lo establecido en el apartado anterior se entenderá sin perjuicio de lo previsto en el apartado 2 del artículo 9 de la Ley 41/2002 (...) en los términos que reglamentariamente se determinen*"; Artículo 9, LBAP: "*Límites del consentimiento informado y consentimiento por representación.*
2. Los facultativos podrán llevar a cabo las intervenciones clínicas indispensables a favor de la salud del paciente, sin necesidad de contar con su consentimiento, en los siguientes casos: a) Cuando existe riesgo para la salud pública a causa de razones sanitarios establecidas por la Ley. En todo caso, una vez adoptadas las medidas pertinentes, de conformidad con lo establecido en la Ley Orgánica 3/1986, se comunicarán a la autoridad judicial en el plazo máximo de 24 horas siempre que dispongan el internamiento obligatorio de personas; b) Cuando existe riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir su autorización, consultando, cuando las circunstancias lo permitan, a sus familiares o a las personas vinculadas de hecho a él"; Artículo 7.4 RD 223/2004, de 6 de febrero, por el que se regulan los Ensayos Clínicos con Medicamentos: "*Cuando el ensayo clínico tenga un interés específico para la población en la que se realiza la investigación y lo justifiquen razones de necesidad en la administración del medicamento en investigación, podrá someterse a un sujeto a un ensayo clínico sin obtener el consentimiento previo en los siguientes casos: a) Si existe un riesgo inmediato grave para la integridad física o psíquica del sujeto, se carece de una alternativa terapéutica apropiada en la práctica clínica y no es posible obtener su consentimiento o el de su representante legal. En este caso, siempre que las circunstancias lo permitan, se consultará previamente a las personas vinculadas a él por razones familiares o de hecho. b) Si el sujeto no es capaz para tomar decisiones debido a su estado físico o psíquico y carece de representante legal. En este caso, el consentimiento lo prestarán las personas vinculadas a él por razones familiares o de hecho.*
En ambos casos, esta eventualidad y la forma en que se procederá debe hallarse prevista en la documentación del ensayo aprobada por el Comité Ético de Investigación Clínica, y el sujeto o su representante legal será informado en cuanto sea posible y deberá otorgar su consentimiento para continuar en el ensayo si procediera"; Artículo 21 Ley 14/2007, de 3 de julio, de Investigación Biomédica:"*Investigación en personas incapaces de consentir debido a su situación clínica.*

El caso que se acaba de ver se refiere a cuando un sujeto se somete a una intervención con fines de investigación. Los datos se recogen de la propia operación y el principio de autonomía prima, en la gran mayoría de casos, sobre los intereses de quienes realizan las investigaciones. Como se ha dicho, otra cosa será que la información recabada pueda emplearse posteriormente, una vez contenida en los ficheros obrantes en un sistema sanitario, con los más diversos fines: control de gastos, de gestión puramente administrativa, de inspección, otras investigaciones, etc. Estas realidades se analizarán en el apartado dedicado a la cesión.

D) Por último, más allá de los supuestos de investigación, pueden encontrarse otros fines para los que el tratamiento de datos de salud resulta necesario. Se está hablando de la manipulación de datos con fines administrativos, de gestión o de inspección. En estos supuestos también entran en colisión el derecho a la autodeterminación informativa y el derecho a la protección de la salud. No cabe duda de que las funciones administrativas de los centros son necesarias para desarrollar una eficiente actividad sanitaria.

La mayoría de las veces estos datos son recabados a través de cesiones o accesos a ficheros sanitarios ya existentes. Piénsese, por ejemplo, en los casos en que se realiza una actividad inspectora por parte de la Administración sanitaria, en la que la recopilación de información se llevará a cabo mediante el acceso de los agentes a ficheros ya obrantes en otros departamentos de la propia Administración. Lo mismo ocurre cuando se trata realizar un control de los gastos realizados por un departamento concreto. El análisis de estas circunstancias se llevará a cabo en el apartado dedicado a las cesiones.

III.4.4.D. Excepciones al consentimiento en la recogida de datos sanitarios. Especial referencia a las intervenciones corporales no consentidas.

III.4.4.D.a. Exposición de los supuestos en que es posible realizar intervenciones corporales sin consentimiento del paciente. Distinción entre los casos en que el paciente está consciente o inconsciente.

En el ámbito sanitario la recogida de datos relativos a los pacientes y usuarios, sea para fines sanitarios o administrativos, se realizará, como norma general, cuando éstos los remitan de manera voluntaria[1839]. Se ha comentado que, a pesar de la referencia de la LBAP al deber de los pacientes y usuarios de transmitir la información necesaria para llevar a cabo las actividades

1. Para la realización de una investigación en situaciones clínicas de emergencia, en las que la persona implicada no pueda prestar su consentimiento, deberán cumplirse las siguientes condiciones específicas: a) Que no sea posible realizar investigaciones de eficacia comparable en personas que no se encuentren en esa situación de emergencia. b) Que en el caso de que no sea previsible que la investigación vaya a producir resultados beneficiosos para la salud del paciente, tenga el propósito de contribuir a mejorar de forma significativa la comprensión de la enfermedad o condición del paciente, con el objetivo de beneficiar a otras personas con la misma enfermedad o condición, siempre que conlleve el mínimo riesgo e incomodidad para aquél. c) Que la autorización de la investigación se ponga en conocimiento del Ministerio Fiscal. (...)".

[1839] LÓPEZ, MOYA, MARIMÓN y PLANAS, *Protección de Datos...,* cit., 2001, p. 11: "Con relación a la recogida de los datos, si entendemos que esta actividad queda fuera del término <<tratamiento>>, la Ley no establece que sea preciso un consentimiento previo del interesado para recabar los datos; de hecho, el paciente está consintiendo la recogida desde el momento que él mismo facilita los datos o se somete a la realización de una determinada prueba diagnóstica para obtenerlos".

asistenciales pertinentes, no parece que se pueda forzar a nadie para que transmita información sanitaria con la finalidad de proteger su salud. En los centros la información sanitaria se recaba normalmente bien porque los usuarios la transmiten oralmente o de forma escrita en una consulta, o porque permiten que se realicen intervenciones sobre su cuerpo, sin que se fuerce a nadie a transmitirla para que sea tratada posteriormente. En la medida en que el usuario autoriza las operaciones sanitarias que le van a realizar o transmite voluntariamente la información, consiente la recogida de los datos[1840]. La necesidad de que sea el paciente quien autorice dichas operaciones se basa en el principio de autonomía[1841], y en caso de negarse a transmitir cierta información tendrá que ser el propio paciente quien asuma las consecuencias.

La recogida de datos de salud necesita, de inicio, del consentimiento de su titular. Sin embargo, en las diferentes actuaciones que completan la genérica finalidad de proteger la salud: asistencia, situaciones de urgencia, investigaciones, protección de la salud pública, podría plantearse la posibilidad de que el paciente se vea sometido a intervenciones corporales sin que se cuente con su autorización o, incluso, que sean contrarias a su voluntad. A falta de una transmisión voluntaria de datos por parte del paciente, podría plantearse si existen situaciones en que se puede utilizar la fuerza para extraer determinada información sobre su salud. Evidentemente este tipo de intervenciones llevaría a la recogida de información sobre la salud de un sujeto sin mediar consentimiento del mismo. Esto último, hay que recordar, no quiere decir que no se haya de dar la información oportuna a dichos pacientes sobre las características que rodearán al tratamiento de sus datos.

La LBAP, siguiendo en cierta medida lo que ya disponía la LGS[1842], señala que se podrán realizar intervenciones clínicas sin consentimiento cuando exista riesgo para la salud pública a causa de razones sanitarias establecidas por la Ley, o riesgo inmediato grave para la integridad física o psíquica del enfermo y no es posible conseguir la autorización oportuna, consultando, cuando sea posible, a familiares o personas vinculadas de hecho al paciente[1843]. Esta regulación se ha seguido posteriormente, también, en la Ley de Investigación Biomédica en relación a la obtención de muestras biológicas del cuerpo del propio sujeto[1844]. De ese precepto podrían

[1840] APDCM, *Guía de Protección...,* cit., 2004, p. 288-290; SÁNCHEZ CARO y SÁNCHEZ CARO, *El Médico…,* cit., 2001, p. 136; SÁNCHEZ CARO y ABELLÁN, *Telemedicina y Protección...,* cit., 2002, p. 63-64.

[1841] STC 24 de septiembre 2007, FJ 3. MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 26.

[1842] Artículo 10 LGS: "*Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias: (...) 6. A la libre elección entre las opciones que le presente el responsable médico de su caso, siendo preciso el previo consentimiento escrito del usuario para la realización de cualquier intervención, excepto en los siguientes casos: a) Cuando la no intervención suponga un riesgo para la salud pública; b) Cuando no esté capacitado para tomar decisiones, en cuyo caso, el derecho corresponderá a sus familiares o personas a él allegadas; c) Cuando la urgencia no permita demoras por poderse ocasionar lesiones irreversibles o existir peligro de fallecimiento*".

[1843] Artículo 9.2 LBAP.

[1844] Artículo 58 Ley 14/2007, 3 de julio de 2007, de Investigación Biomédica: "*1. La obtención de muestras biológicas con fines de investigación biomédica podrá realizarse únicamente cuando se haya obtenido previamente el consentimiento escrito del sujeto fuente y previa información de las consecuencias y los riesgos que pueda suponer tal obtención para su salud. Dicho consentimiento será revocable.*

2. El consentimiento del sujeto fuente será siempre necesario cuando se pretendan utilizar con fines de investigación biomédica muestras biológicas que hayan sido obtenidas con una finalidad distinta, se proceda o no a su anonimización.

No obstante lo anterior, de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea

deducirse diferentes alternativas. El sujeto sobre el que se pueden llevar a cabo las intervenciones puede encontrarse ante dos situaciones. En primer lugar, podría estar en un estado de inconsciencia o incapacidad en que no fuera capaz de dar o emitir su consentimiento. En esta situación, la protección de la salud pública o la salvaguarda de la salud individual podrían justificar una intervención sin necesidad de recoger autorización alguna. En segundo lugar, podría situarse en una circunstancia en que es consciente y capaz para emitir su consentimiento. En este estado, cabe plantearse si la protección de la salud pública o individual pueden justificar una intervención, incluso contraria a la voluntad del paciente, forzando al sujeto a sufrir o padecer dicha operación.

Atendiendo a la letra de la Ley parece que el primer supuesto es perfectamente asumible. Cuando el paciente se encuentra en un estado en que no es capaz de emitir su consentimiento pueden darse diferentes situaciones. Primero, puede suceder que exista un "riesgo inmediato grave para la integridad física o psíquica" del paciente, que éste no tenga capacidad para consentir un tratamiento y no se pueda consultar a los familiares o personas vinculadas de hecho a él. En estos casos no parece haber problema para que se actúe sin recabar el consentimiento del afectado. La única incertidumbre surgiría a la hora de decidir si existe un riesgo grave e inmediato para la salud de una persona. Este peligro inmediato podría equipararse con el concepto de urgencia vital. Interpretado en un sentido literal, la urgencia vital se refiere al supuesto en que la vida está en peligro. Sin embargo, en la práctica tiene un sentido más amplio. La urgencia vital ha de entenderse como estado que requiere acción terapéutica inmediata que, de no darse, supondría un importante peligro para la salud de la persona. Así, se ha definido por la jurisprudencia como la existencia de un riesgo inminente de vida o pérdida de órganos o miembros fundamentales para el desarrollo normal del vivir[1845], y se caracteriza, en la mayoría de los casos, porque en ella está en riesgo la vida del afectado[1846]. Si bien el riesgo inmediato para la integridad física o psíquica puede abrazar algún supuesto más, la definición dada sobre la urgencia vital ayuda a entender que no siempre se puede aplicar la excepción al consentimiento cuando el paciente esté inconsciente[1847]. Segundo, podría ocurrir que, estando el paciente en la citada situación de gravedad e incapacidad para decidir por sí mismo, sí se pudiera localizar al familiar o allegado. En este caso podrían suceder dos cosas. Que este último consintiera el tratamiento propuesto por los facultativos o que se opusiera. En el primer caso no habría problema alguno. En cuanto al segundo, se entiende que hay argumentos suficientes para concluir que los profesionales sanitarios pueden imponer su criterio a la negativa de los

posible o represente un esfuerzo no razonable en el sentido del artículo 3.i de esta Ley. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente, el cual deberá tener en cuenta, como mínimo, los siguientes requisitos:
a..Que se trate de una investigación de interés general.
b.Que la investigación se lleve a cabo por la misma institución que solicitó el consentimiento para la obtención de las muestras.
c.Que la investigación sea menos efectiva o no sea posible sin los datos identificativos del sujeto fuente.
d.Que no conste una objeción expresa del mismo.
e.Que se garantice la confidencialidad de los datos de carácter personal". A este respecto ROMEO CASABONA, "La protección de datos…", cit., 2009, p. 58.
[1845] SSTS 15 de octubre 1987, FJ 2 y 21 de diciembre 1988, FJ 5.
[1846] STS 31 de mayo 1995.
[1847] SAN 19 de enero de 2005, FJ 5.

familiares, siempre que se adopten las garantías oportunas que más adelante se señalarán, como la autorización judicial[1848]. Hay que tener en cuenta que la LBAP, al referirse a los familiares o las personas vinculadas de hecho al paciente, lo hace para exigir que sean consultados cuando sea posible. No parece que en la Ley se esté otorgando a estos representantes la facultad de negar un tratamiento médico en nombre de un paciente inconsciente o carente de la capacidad de tomar una tal decisión, sino, simplemente, un derecho a ser consultados. Tercero, cuando esté en juego la salud pública. En este caso ocurre lo mismo. No siempre que haya de protegerse este bien jurídico y el paciente se encuentre en dicho estado puede aplicarse la excepción, sino que será necesario que la salud pública esté en grave e inminente riesgo.

La segunda situación planteada genera mayores problemas interpretativos. Se está haciendo referencia al caso en que se fuerza a un sujeto a sufrir o padecer una intervención, en contra de su voluntad. La posibilidad de emplear la *vis física* para llevar a cabo intervenciones ha sido puesta en duda[1849]. No obstante, atendiendo al ordenamiento parece que en algún caso puede tener cabida.

La intervención corporal podría definirse, dejando a un lado los matices que puedan fijarse desde el ámbito penal, como el empleo del propio cuerpo como fuente de información sobre el estado de salud de una persona[1850]. Se comprende, en contra de lo que se ha reconocido por algunos autores y cierta jurisprudencia[1851], el concepto de intervención en un sentido amplio[1852], que abraza también meras inspecciones o registros corporales, que sin conllevar un menoscabo directo del cuerpo también pueden suponer una afección al derecho a la autodeterminación, caso por ejemplo de pruebas radiológicas[1853].

La figura de la intervención coactiva es especialmente compleja, pues entran en juego diferentes bienes jurídicos[1854]. Derechos como la intimidad corporal, la integridad física de las personas[1855] o el derecho a la libertad de movimiento[1856], el derecho a no declarar contra uno

[1848] COBREROS MENDAZONA, *Los tratamientos sanitarios…*, cit., 1988, pp. 292-293.
[1849] ÁLVAREZ DE NEYRA KAPPLER, *La prueba de ADN…,* cit., 2008, p. 77; STS 4 de febrero de 2003, FJ 3.
[1850] GÓMEZ AMIGO, *Las Intervenciones Corporales…,* cit., 2003, pp. 25-37; GARCÍA VILA, "Los cacheos…", cit., 2000; ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 32.
[1851] ORTEGO PÉREZ, "Problemas derivados…", cit., 2004. STC 16 de diciembre de 1996, FJ 2: distingue entre las inspecciones y registros corporales y las intervenciones corporales: "Las denominadas inspecciones y registros corporales, consistentes en <<cualquier género de reconocimiento del cuerpo humano, bien sea para la determinación del imputado (…) o de circunstancias relativas a la comisión del hecho punible (…) o para el descubrimiento del delito". Señala que "La otra clase de medidas son las propiamente denominadas intervenciones corporales, consistentes (…)<<en la extracción del cuerpo de determinados elementos externos o internos para ser sometidos a informe pericial (análisis de sangre, orina, pelos, uñas, biopsias, etc.) o en su exposición a radiaciones (…) con objeto también de averiguar determinadas circunstancias relativas a la comisión del hecho punible o a la participación en él del imputado>>".
[1852] MAGRO SERVET, "La actuación policial…", cit., 2001.
[1853] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, pp. 35y 60-61; MAGRO SERVET, "La actuación policial…", cit., 2001.
[1854] GARCÍA VILA, "Los cacheos…", cit., 2000.
[1855] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, pp. 207-208.
[1856] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 489.

mismo[1857] e incluso, en algunos casos, a la libertad ideológica o religiosa del afectado[1858], podrían verse vulnerados.

A los citados derechos del paciente se les opondrían otros como el propio derecho a la salud de la persona, que en algunos casos llega a identificarse con el derecho a la vida, el derecho a la salud de otras personas, o la libertad de conciencia del profesional sanitario que puede verse ante la situación de tener que hacer algo ante un paciente que no quiere ser tratado y cuya vida está en juego, e incluso el derecho de este profesional a realizar su trabajo de manera eficiente. No hay que olvidar, que los derechos del paciente tienen su límite también en los derechos del profesional sanitario[1859].

No corresponde aquí realizar un análisis exhaustivo sobre las confrontaciones que pueden producirse entre los diferentes bienes jurídicos citados. Como se puede imaginar, la resolución de estos conflictos, desde el punto de vista jurídico, exige un debate que excede la intención de este trabajo. Bastará con apuntar una serie de criterios que ayuden a comprender, desde el punto de vista del derecho a la autodeterminación informativa, cuándo se pueden llevar a cabo estas operaciones. Hay que recordar que estas intervenciones conllevarán la recogida de datos de salud sin consentimiento del titular, por lo que afectarán al derecho fundamental que aquí se analiza.

Del ordenamiento pueden deducirse una serie de criterios que ayuden a resolver el problema expuesto. Se identifican diferentes normas que incorporan en su articulado supuestos en que parece posible llevar a cabo intervenciones sin contar con el consentimiento del titular. Ya se ha citado la LBAP. En la más reciente normativa sanitaria autonómica también se recoge la misma posibilidad[1860]. La misma línea interpretativa sigue La Ley de Prevención de Riesgos

[1857] Artículo 24.2 CE.
[1858] STC 29 de mayo del 2000, FJ 4.
[1859] STC 29 de mayo del 2000, FJ 4: "el derecho que asiste al creyente de creer y conducirse personalmente conforme a sus convicciones no está a más límites que los que imponen el respeto a los derechos fundamentales ajenos y otros bienes jurídicos protegidos constitucionalmente".
[1860] Ley Foral 17/2010, 8 de noviembre de 2010, de Derechos y Deberes de las Personas en materia de Salud en la Comunidad Foral de Navarra, Artículo 6 "*Intervenciones públicas sobre personas.*
Conforme establece la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública, las autoridades sanitarias podrán llevar a cabo las siguientes intervenciones públicas en los supuestos de riesgos para la salud de terceras personas:
1. Medidas de reconocimiento, diagnóstico, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad.
2. A fin de controlar las enfermedades transmisibles, además de realizar las acciones preventivas generales, podrán adoptar las medidas oportunas para el control de las personas enfermas, de las que estén o hayan estado en contacto con ellas y del medio inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible, de acuerdo con la evidencia científica sobre su necesidad.
3. Las medidas anteriores deben adoptarse respetando los derechos que la Constitución reconoce a los ciudadanos, especialmente el derecho a la integridad física y moral, así como a la intimidad personal, de acuerdo con lo establecido por la normativa de protección de datos de carácter personal y con los procedimientos que esta normativa y las demás normas aplicables hayan establecido, y disponiendo de las autorizaciones preceptivas".
Artículo 7: "*Derecho a la información y limitaciones al derecho de previo consentimiento.*
Sin perjuicio de facilitar a la persona una información completa y veraz, son situaciones de excepción a la exigencia de previa obtención de consentimiento para realizar las intervenciones clínicas indispensables en favor de la salud de

Laborales[1861]. La protección de la salud del trabajador o de los demás trabajadores puede llevar a justificar la realización de reconocimientos médicos sin necesidad de consentimiento. En el ámbito penal se admite también la posibilidad de llevar a cabo este tipo de operaciones con el fin de perseguir determinados delitos, en la medida en que se cuente con autorización judicial[1862].

Precisamente en esta última disciplina jurídica las normas no parecen dejar lugar a dudas de que la intervención corporal forzosa o coactiva resulta en determinados casos una operación necesaria en beneficio del interés general. Si bien es verdad que se han planteado dudas sobre el alcance de dichas operaciones y el procedimiento que han de seguir, resulta comúnmente admitido que hay supuestos en que se pueden llevar a cabo cuando el fin es la prevención o

la persona afectada, la existencia de riesgo serio para la salud pública, si así lo exigen razones sanitarias de acuerdo con lo que establece la legislación que sea de aplicación".
Artículo 8: "*Limitaciones en las intervenciones públicas sobre personas en garantía de sus derechos.*
Las intervenciones públicas especificadas en el artículo 6 se sujetarán a las siguientes reglas:
a) Preferencia de la colaboración voluntaria con las autoridades sanitarias.
b) Obtención previa de autorización judicial o, en su caso, ratificación judicial, conforme a la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa, para la adopción de las medidas que las autoridades sanitarias consideren urgentes y necesarias para la salud pública y que impliquen privación o restricción de la libertad o de otros derechos fundamentales de las personas. En todo caso, una vez adoptadas las medidas sanitarias o administrativas, de conformidad con lo establecido en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en materia de Salud Pública, deberán ser comunicadas a la autoridad judicial en el plazo máximo de 24 horas, cuando supongan el internamiento obligatorio de las personas.
c) Minimización de la incidencia sobre la libre circulación de personas.
d) Prohibición de ordenar medidas obligatorias que supongan riesgo para la vida.
e) Proporcionalidad de las intervenciones a los fines que en cada caso se persigan".

[1861] Artículo 22.1 Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales: "*El empresario garantizará a los trabajadores a su servicio la vigilancia periódica de su estado de salud en función de los riesgos inherentes al trabajo.*
Esta vigilancia sólo podrá llevarse a cabo cuando el trabajador preste su consentimiento. De este carácter voluntario sólo se exceptuarán, previo informe de los representantes de los trabajadores, los supuestos en los que la realización de los reconocimientos sea imprescindible para evaluar los efectos de las condiciones de trabajo sobre la salud de los trabajadores o para verificar si el estado de salud del trabajador puede constituir un peligro para el mismo, para los demás trabajadores o para otras personas relacionadas con la empresa o cuando así esté establecido en una disposición legal en relación con la protección de riesgos específicos y actividades de especial peligrosidad"; CARDONA RUBERT, *Informática y Contrato…,* cit., 1999, pp. 180-184; STC 15 de noviembre de 2004, FFJJ 5 y 6.

[1862] Artículo 326 LECrim: "(…) *Cuando se pusiera de manifiesto la existencia de huellas o vestigios cuyo análisis biológico pudiera contribuir al esclarecimiento del hecho investigado, el Juez de Instrucción adoptará u ordenará a la Policía Judicial o al médico forense que adopte las medidas necesarias para que la recogida, custodia y examen de aquellas muestras se verifique en condiciones que garanticen su autenticidad, sin perjuicio de lo establecido en el artículo 282*"; Artículo 363 LECrim: "*(...) Siempre que concurran acreditadas razones que lo justifiquen, el Juez de Instrucción podrá acordar, en resolución motivada, la obtención de muestras biológicas del sospechoso que resulten indispensables para la determinación de su perfil de ADN. A tal fin, podrá decidir la práctica de aquellos actos de inspección, reconocimiento o intervención corporal que resulten adecuados a los principios de proporcionalidad y razonabilidad*"; DA 3 LO 10/2007, de 8 de octubre, reguladora de la Base de Datos Policial sobre Identificadores Obtenidos a partir del ADN : "*Para la investigación de los delitos enumerados en la letra a del apartado 1 del artículo 3, la policía judicial procederá a la toma de muestras y fluidos del sospechoso, detenido o imputado, así como del lugar del delito. La toma de muestras que requieran inspecciones, reconocimientos o intervenciones corporales, sin consentimiento del afectado, requerirá en todo caso autorización judicial mediante auto motivado, de acuerdo con lo establecido en la Ley de Enjuiciamiento Criminal*"; ETXEBARRIA GURIDI, "La LO 10/2007…", cit., 2008; ETXEBARRIA GURIDI, "Los análisis de ADN…", cit., 2004.

investigación de delitos[1863]. Aunque no se refiera al ámbito estrictamente penal, también se ha admitido la intervención cuando es la única fórmula de conocer la paternidad de una persona[1864].

En los casos que se acaban de citar se ha entendido que para poder llevar a cabo la intervención corporal, como forma de extraer información sobre un determinado sujeto sin necesidad de recabar su consentimiento, se deberán cumplir tres requisitos: el respeto al principio de proporcionalidad, la previsión por parte de la Ley del supuesto en que puede exceptuarse el consentimiento y la existencia de una autorización judicial justificando la medida[1865]. Estos requisitos serán analizados a continuación someramente, vinculados a las intervenciones realizadas con el fin de proteger la salud de las personas.

III.4.4.D.b. Sobre la posibilidad de realizar intervenciones corporales forzosas en el ámbito sanitario.

En el ámbito sanitario la posibilidad de obligar a un sujeto a recibir un tratamiento que consista en una intervención corporal con el fin de proteger su salud plantea serias dudas. Se ha apuntado que la LBAP reconoce la posibilidad de realizar intervenciones sin el consentimiento del titular. Esta previsión podría llevar a admitir que en estos casos se puede forzar a un sujeto a someterse a dichas operaciones, incluso contra su voluntad. Se adelanta desde ahora que esto no siempre es así. La norma dispone que se "podrán" realizar las intervenciones sin consentimiento, pero esto no quiere decir que pueda forzarse a nadie a ser objeto de las mismas. La Ley se refiere aquí a los casos en que el sujeto está incapacitado física o jurídicamente para dar su consentimiento y su salud corre un riesgo grave e inmediato. El propio precepto señala que el límite entrará en juego cuando no sea posible recabar la autorización del particular, por lo que cuando sea posible deberá contarse con dicha autorización[1866]. Las intervenciones deberán ser consentidas cuando el paciente está capacitado para expresar su voluntad.

Ya se ha dicho que en la actualidad el principio de autonomía de los pacientes ha adquirido gran relevancia en la normativa sanitaria[1867]. El sujeto capacitado e informado es capaz de tomar sus propias decisiones sobre lo que le concierne: su salud, los datos relativos a su persona…[1868] Ejemplo claro del reconocimiento de ese principio de autonomía en la actualidad es la figura de las instrucciones previas. La LBAP regula este instrumento[1869]. Como ya se dijera, a través de estas instrucciones el paciente puede determinar qué tipo de tratamiento médico quiere recibir en

[1863] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, pp. 34-35.
[1864] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 474; SÁNCHEZ CARO y SÁNCHEZ CARO, *El Médico...,* cit., 2001, pp. 85 y 86 en relación al ATC 221/1990, de 31 de mayo y la STC 7/1994, de 17 de enero; ROMERO COLOMA, "Pruebas biológicas de paternidad…", cit,. 2009; ROMERO COLOMA, *Identidad genética…,* cit., 2009, pp. 158-159, afirma que ha de prevalecer el derecho a la investigación de la paternidad sobre el derecho a la intimidad.
[1865] STC 24 de septiembre de 2007, FJ 6 y 8.
[1866] ARRUEGO, "La naturaleza constitucional…", cit., 2008, p. 80; LIZARRAGA BONELLI, "La Información...", cit., 2004, pp. 293-295.
[1867] ARRUEGO, "La naturaleza constitucional…", cit., 2008, p. 67.
[1868] SAP de Madrid 28 de enero de 2008, FJ 1.
[1869] Artículo 11 LBAP: "*1. Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. (...)*".

un futuro. Así, por ejemplo, puede exigir que no se alargue su vida de manera artificial o contraria a la propia dignidad de la persona[1870].

Con lo dicho hasta ahora pudiera parecer que la autonomía del paciente es inquebrantable en el ámbito sanitario y que no se puede obligar a un sujeto a ser objeto de una intervención. Frente a esta consideración pueden plantearse argumentos válidos. La Ley exige que las instrucciones previas respeten el ordenamiento y no sean contrarias a las leyes[1871]. En este sentido, hay que recordar que el código penal prohíbe la eutanasia activa directa[1872]. Parece comúnmente admitido, a pesar del cambio que está experimentando la configuración y contenido del derecho a la vida[1873], que las instrucciones previas no pueden encubrir un suicidio asistido[1874]. Si el suicidio asistido está prohibido, se entiende que el alcance de la autonomía del paciente se encuentra limitado. Siendo esto así, se plantea si de esta previsión puede deducirse algún supuesto en que la actuación del profesional se imponga a la voluntad del paciente de no recibir un tratamiento determinado.

De lo que se ha expuesto podrían darse argumentos favorables a la posición que admite la intervención forzosa con motivos sanitarios y también a la contraria. Sin embargo, se entiende que está en la voluntad del legislador dar prioridad a la autonomía del particular, frente a su derecho a la protección de la salud.

No es esta una materia que haya sido analizada extensamente por la jurisprudencia. No obstante, de alguna resolución pueden extraerse conclusiones de interés. Concretamente, los tribunales analizaron un caso en que se obligaba a una serie de presos en huelga de hambre a someterse a un tratamiento para salvar sus vidas. De esta jurisprudencia se desprenden unos criterios que ayudan a comprender en qué casos puede obligarse a un sujeto a someterse a intervenciones en contra de su voluntad. Se señala en esta sentencia que al tratarse de presos se encuentran en una situación de sujeción especial. Esta circunstancia hace, según los tribunales, que los derechos de estas personas puedan verse limitados en mayor medida que los de los sujetos que no se encuentran en esa situación[1875]. De esta forma, y teniendo en cuenta que la situación de urgencia terapéutica ha sido creada por los propios pacientes presos con el

[1870] MESTRE DELGADO, "EL caso <<Eluana Englaro>>…", cit., 2009; DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, pp. 106-107

[1871] Artículo 11.3 LBAP: "*No serán aplicadas las instrucciones previas contrarias al ordenamiento jurídico, a la <<lex artis>>, ni las que no se correspondan con el supuesto de hecho que el interesado haya previsto en el momento de manifestarlas. EN la historia clínica del paciente quedará constancia razonada de las anotaciones relacionadas con estas previsiones*".

[1872] Artículo 143 CP: "1. *El que induzca al suicidio de otro será castigado con la pena de prisión de cuatro a ocho años. 2. Se impondrá la pena de prisión de dos a cinco años al que coopere con actos necesarios al suicidio de una persona. 3. Será castigado con la pena de prisión de seis a diez años si la cooperación llegara hasta el punto de ejecutar la muerte. 4. El que causare o cooperare activamente con actos necesarios y directos a la muerte de otro, por la petición expresa, seria e inequívoca de éste, en el caso de que la víctima sufriera una enfermedad grave que conduciría necesariamente a su muerte, o que produjera graves padecimientos permanentes y difíciles de soportar, será castigado con la pena inferior en uno o dos grados a las señaladas en los números 2 y 3 de este artículo*"; DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, pp-. 100-102.

[1873] CHUECA RODRÍGUEZ, "El Marco Constitucional…", cit., 2009.

[1874] VILLAR ABAD, "La regulación de las instrucciones…", cit., p. 323; SILVA SÁNCHEZ, "Los <<Documentos de Instrucciones Previas>>…", cit., 2003.

[1875] STC 19 de julio de 1990, FJ 4.

fin de llevar a cabo una reivindicación, se justifica que la actuación de los profesionales sanitarios se imponga sobre la autonomía y voluntad de las personas presas. Sin embargo, la propia sentencia concluye que fuera de esos supuestos o circunstancias especiales no cabe la intervención obligatoria o coactiva[1876]. Siguiendo esta línea interpretativa se entendería que en una situación común, en que un paciente enfermo de gravedad acude a un centro y se niega a un tratamiento, hay que respetar su voluntad.

Se ha afirmado por parte de los tribunales que el derecho a la vida constituye un valor superior, fundamento de los demás derechos y bienes[1877], y que no reconoce a su vez el derecho a la propia muerte[1878]. Frente a este argumento, tal y como se establecía en el voto particular de la citada resolución, cabe apuntar que la intervención coactiva afecta al núcleo mismo de la libertad o autonomía de la persona[1879]. A pesar de que pueda parecer contradictorio, pese a no reconocerse el derecho a la propia muerte, la libertad alcanza la facultad de disponer de la salud de cada uno, incluso cuando la vida está en juego. Así, cuando un sujeto se niega a recibir un tratamiento determinado, incluso cuando su vida está en peligro, el profesional sanitario deberá respetar su voluntad[1880]. La mera negativa del paciente a someterse a un tratamiento bastará para que su voluntad se vea respetada, cuando lo que esté en juego sea su propia salud[1881]. Tanto en los supuestos de medicina voluntaria como en los casos de medicina necesaria, en la que el paciente tiene menos alternativas de elección, la autonomía del sujeto ha de ser respetada[1882]. Esta misma conclusión parece deducirse de una resolución más reciente del máximo intérprete de la Constitución[1883], en la que se señala que el rechazo a un tratamiento médico determinado que puede conducir a la muerte constituye el mero ejercicio de la autodeterminación.

Parece, por lo tanto, que no cabe la intervención corporal coactiva cuando la finalidad de la acción es la protección de la salud del sujeto que se opone al tratamiento. De esta forma, parece claro que en estos supuestos no estará justificada la recogida de datos sanitarios de dicha persona sin su consentimiento, a pesar del fin que se pretende. La oposición del paciente será insalvable.

Cosa distinta ocurre cuando lo que está en juego no es la salud de un particular sino la salud pública[1884]. El bien jurídico protegido en este caso es el interés general. La intervención no se daría simplemente para salvaguardar la salud individual del paciente, sino para proteger un interés común. De esta forma el límite a la autonomía y libertad del particular será posible. Una cosa es que una persona decida sobre su propia salud y otra que lo haga sobre la salud de las

[1876] STC 19 de julio de 1990, FJ 4.
[1877] STC 11 de abril de 1985, FJ 2.
[1878] STC de 27 de junio de 1990, F 7: "el derecho fundamental a la vida tiene un contenido de protección positiva que impide configurarlo como un derecho de libertad que incluya el derecho a la propia muerte".
[1879] Voto Particular del Magistrado Jesús Leguina Villa, STC 19 de julio de 1990.
[1880] COBREROS MENDAZONA, *Los tratamientos sanitarios…*, cit., 1988, p. 318; LAMARCA PÉREZ, "Autonomía de la voluntad…", cit., 2009.
[1881] ARRUEGO, "La naturaleza constitucional…", cit., 2008, p. 79.
[1882] STSJ de Galicia 2 de julio de 2008, FJ 5.
[1883] STC 18 de julio de 2002.
[1884] COBREROS MENDAZONA, *Los tratamientos sanitarios…*, cit., 1988, p. 299; LAMARCA PÉREZ, "Autonomía de la voluntad…", cit., 2009.

demás personas. No hay que perder de vista el principio que consagra la CE de que el libre desarrollo de la personalidad de cada uno ha de cohonestarse con el respeto a los derechos de los demás[1885]. Recientemente se han pronunciado los tribunales a este respecto, obligando a diferentes niños a vacunarse contra el sarampión con el fin de evitar un brote epidémico, en una decisión que no tenía precedentes[1886]. Para realizar esta operación será necesario que se den las circunstancias que justificaban en el ámbito penal la intervención corporal forzosa. Debe respetarse el principio de proporcionalidad, el límite ha de preverse en una norma con rango legal y debe reconocerse en el caso concreto por autorización judicial la posibilidad de aplicar la excepción. La normativa sanitaria navarra recoge también estos requisitos, como preceptivos para llevar a cabo intervenciones inconsentidas[1887].

A) El respeto al principio de proporcionalidad es necesario por cuanto se trata de limitar un derecho fundamental[1888]. Este principio ya fue analizado con detenimiento más arriba. Exige que se valore si el límite a la autonomía del paciente constituye una medida justificada para conseguir un fin determinado; en el conflicto que aquí se estudia la salvaguarda de su salud pública. Para ello es necesario ver si la intervención corporal constituye un medio adecuado, necesario y proporcional en sentido estricto para conseguir dicho fin[1889]. Como ya se ha analizado, la intervención y la consiguiente recogida y manipulación de información es esencial en el ámbito sanitario para salvaguardar ese interés general. El daño que se causaría si no se trataran esos datos podría ser mayor que el evitado[1890]. Es por ello por lo que se entiende que la intervención corporal puede considerarse un medio proporcional para el cumplimiento de dicho fin, siempre que se respeten unas garantías. La intervención será la estrictamente necesaria para la salvaguarda de la salud pública[1891]. En este sentido, solamente se recabarán los datos que se estimen necesarios para obtener el fin que se persigue.

Hay que recordar que el principio de proporcionalidad consiste en el análisis de la relación entre medio y fin. En este sentido, el elemento principal a analizar, que justificará la limitación del consentimiento, será la finalidad concreta que se pretende conseguir. Como se afirmara, las excepciones al consentimiento se fundamentan en el cumplimiento de determinadas finalidades. En este caso, la excepción al derecho a autorizar la intervención corporal deberá estar justificada por la persecución de un fin concreto[1892]. Teniendo en cuenta la relevancia del bien jurídico

[1885] Artículo 10.1 CE. COBREROS MENDAZONA, *Los tratamientos sanitarios…*, cit., 1988, p. 359.
[1886] AJCA de Granada 24 de noviembre de 2010, en el que se justifica la pertinencia de la actuación de la Administración basándose, fundamentalmente, en la LO 3/1986 de 4 de abril, sobre Medidas Especiales en Materia de Salud Pública. "El Juez autoriza la vacunación forzosa de niños contra el Sarampión en Granada", *El País,* 25 de noviembre de 2010; "Un juez ordena a 35 niños que se vacunen del sarampión", *Público,* 25 de noviembre de 2010.
[1887] Artículo 8 Ley Foral 17/2010, 8 de noviembre de 2010, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra.
[1888] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, p. 208.
[1889] STC 16 de diciembre de 1996, FJ. 6.
[1890] DE LORENZO Y MONTERO, *Derechos y Obligaciones...,* cit., 2003, p. 58.
[1891] STC 27 de junio de 1990, FJ 8
[1892] STC 24 de septiembre de 2007, FJ 4, donde dice que "las intervenciones corporales pueden conllevar una intromisión en el ámbito constitucionalmente protegido del derecho a la intimidad personal, no tanto por el hecho en sí de la intervención (que, en su caso, afecta al derecho a la integridad física), sino por razón de su finalidad, es decir, por lo que a través de ellas se pretenda averiguar, si se trata de información referente a la esfera de la vida privada y que el sujeto puede no querer desvelar, como la relativa al consumo de alcohol o de drogas".

afectado, la autonomía o autodeterminación personal, y las implicaciones que puede conllevar dicha limitación para otros derechos como los más arriba comentados, integridad física, libertad de movimiento, libertad ideológica o religiosa, deberá entenderse que la finalidad que justifique la excepción al consentimiento tendrá que ser de importancia. En el citado ámbito de las investigaciones policiales, para llevar a cabo análisis de ADN sin el consentimiento del sujeto, se requiere, por ejemplo, que se trate de la persecución de delitos de entidad[1893].

No se sabe determinar con exactitud cuál ha de ser el nivel concreto de gravedad que puede justificar esa intervención en el ámbito sanitario. No obstante, atendiendo a la jurisprudencia, parece que se ha de tratar de supuestos especialmente graves[1894]. No hay que olvidar que la dignidad y el libre desarrollo de la personalidad constituyen bienes jurídicos de especial relevancia en la Constitución[1895]. Es por ello por lo que su limitación a través de la excepción al principio de autonomía ha de basarse en intereses jurídicos especialmente relevantes que, en este caso, representarán la salud pública. De esta forma, tiene sentido reconocer la aplicabilidad de la excepción en los casos en que el ordenamiento admite la posibilidad de aplicar medidas especiales para la protección de la salud pública. Se está hablando de los supuestos previstos en la Ley orgánica sobre adopción de medidas especiales para la protección de la salud pública, dirigida a regular esa materia[1896]. Es verdad que esta norma no ha tenido una gran aplicación en la práctica y que no concreta los supuestos en que pueden tomarse esas medidas específicas, pero otorga una vía de validez a las intervenciones coactivas para los casos en que la salud pública está en juego.

B) El segundo requisito lo constituía la necesidad de que una Ley recogiera el supuesto exceptuado[1897]. Se exigía en la normativa y jurisprudencia europea que esta Ley cumpliera con una serie de requisitos, fundamentalmente un determinado grado de claridad. Basta decir en este momento que puede encontrarse fundamento jurídico en normas como la comentada LBAP o la Ley orgánica sobre la adopción de medidas especiales para la protección de la salud pública, en las que se abre la puerta a la intervención sin consentimiento del titular.

C) Como último requisito para llevar a cabo la intervención corporal sin consentimiento del paciente se exige una autorización judicial. Este requisito no se prevé para este caso en la

[1893] ETEBARRIA GURIDI, *La Protección...,* cit., 1998, pp. 196-197.
[1894] STC 19 de julio de 1990, FJ 7: "En todo caso, tal intervención de alimentación forzosa no podrá administrarse sino cuando, según indicación médica, el recluso corra grave y cierto peligro de muerte o de entrar en una situación irreversible"; ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 159.
[1895] Artículo 10.1 CE.
[1896] Artículo 2 LO 3/1986, 14 de abril, de Medidas Especiales en materia de Salud Pública: "*Las autoridades sanitarias competentes podrán adoptar medidas de reconocimiento, tratamiento, hospitalización o control cuando se aprecien indicios racionales que permitan suponer la existencia de peligro para la salud de la población debido a la situación sanitaria concreta de una persona o grupo de personas o por las condiciones sanitarias en que se desarrolle una actividad*"; Artículo 3, LO 3/1986, 14 de abril, de Medidas Especiales en materia de Salud Pública: "*Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible*".
[1897] GÓMEZ AMIGO, *Las Intervenciones Corporales…,* cit., 2003, p. 65.

Constitución como se recoge para otros supuestos en que se limitan derechos fundamentales[1898], pero esto no quiere decir que la autorización judicial no sea necesaria en este ámbito[1899]. Tal como subrayan la Ley[1900], la jurisprudencia[1901] y la doctrina[1902], referidas a la intervención en el ámbito penal, al estar en juego derechos fundamentales de especial relevancia, esta operación requerirá de la citada autorización. En principio, es lógico afirmar que el conflicto entre derechos que se da a la hora de recabar datos de salud a través de una intervención corporal haya de ser resuelta por los órganos judiciales[1903]. Éstos, partiendo de lo que disponen las leyes, determinarán a favor de qué bien jurídico se resuelve el choque concreto[1904]. Es de justicia que no tenga que ser el profesional sanitario quien lleve a cabo este juicio valorativo o ponderativo. A la hora de emitir su autorización el principio de proporcionalidad exigirá que la resolución del choque de bienes haya de llevarse a cabo de manera motivada[1905].

La LBAP cuando se refiere a la posibilidad de llevar a cabo intervenciones sin el consentimiento del titular con el fin de proteger la salud pública, no hace referencia alguna a la necesidad de autorización judicial. Simplemente señala que cuando la medida a adoptar requiera el internamiento de una persona será necesario que el profesional informe de este hecho a la autoridad judicial competente en el plazo de 24 horas[1906]. Como ya se ha indicado, el hecho de que en la norma no se prevea expresamente el requisito de la autorización judicial no quiere decir que no sea exigible, o cuando menos recomendable. La ponderación de los bienes jurídicos en juego debe hacerla un órgano judicial. Otra cosa será que en determinadas situaciones no sea posible recabar dicha autorización. Este requisito puede contar con excepciones.

En lo que concierne a la inviolabilidad domiciliaria, por ejemplo, es la propia Constitución la que dispone el supuesto en que se exceptúa la autorización judicial. Se entiende que no hace falta cuando existe un flagrante delito[1907]. En relación a intervenciones con fines de investigación policial, a pesar de recibir alguna crítica[1908], la jurisprudencia ha interpretado que es posible exceptuar el consentimiento y la autorización judicial cuando se da una situación de urgencia[1909], en la que la solicitud de dicha autorización pudiera entrañar un riesgo en el cumplimiento de la investigación penal, por ejemplo, porque supone una demora.

[1898] Artículo 18.2, CE: "*El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito*"; artículo 18.3, CE: "*Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*".
[1899] ETXEBERRIA GURIDI, *Los Análisis...,* cit., 2000, p. 147.
[1900] Artículo 326 LECrim; Artículo 363 LECrim; DA 3 LO 10/2007, 8 de octubre de 2007, reguladora de la Base de Datos Policial sobre Identificadores Obtenidos a partir del ADN; Artículo 8.b) Ley Foral 17/2010, 8 de noviembre de 2010, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra.
[1901] STS 14 de febrero de 2006, FJ 3; SAN 30 de noviembre de 2005, FJ 1.
[1902] GÓMEZ AMIGO, *Las Intervenciones Corporales…,* cit., 2003, p. 82; MARTÍN PASTOR, "Controversia jurisprudencial…", cit., 2008.
[1903] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, p. 302.
[1904] ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, pp. 257-259 y pp. 266-267.
[1905] ETXEBERRIA GURIDI, *Los Análisis...,* cit., 2000, p. 180.
[1906] Artículo 9.2 LBAP.
[1907] Artículo 18.2 CE.
[1908] GÓMEZ AMIGO, *Las Intervenciones Corporales…,* cit., 2003, p. 83; ETXEBARRIA GURIDI, *Las Intervenciones...,* cit., 1999, pp. 293 y 297.
[1909] STC 16 de diciembre de 1996, FJ 4.

La lógica que se aplica a este supuesto puede ser trasladada al caso que se analiza en este trabajo. Puede entenderse que una intervención corporal llevada a cabo por profesionales sanitarios con el fin de salvaguardar la salud pública, y por lo tanto una recogida de datos, puede desarrollarse sin consentimiento y sin autorización judicial en determinadas circunstancias. Se está pensando en casos en que el cumplimiento del requisito de solicitar una autorización judicial obstaculiza o imposibilita el desarrollo efectivo de las tareas pertinentes. Habrá de tratarse de situaciones de urgencia que hagan imposible la solicitud de esta autorización, incluso verbal. No basta con que se dé una situación de urgencia terapéutica sino que ha de darse también una situación en la que la tramitación de la autorización judicial constituyera un riesgo para el tratamiento médico, por ejemplo, porque retrasaría la actuación médica. Los profesionales sanitarios tendrán la posibilidad de, según los criterios puramente médicos que determinen, decidir si hay que llevar a cabo una intervención urgente o no. En todo caso, se recomienda que una vez realizada la operación se informe cuanto antes sobre la misma a las autoridades judiciales.

CAPÍTULO 5. LA TRANSMISIÓN DE LOS DATOS SANITARIOS.

En este capítulo se van a analizar las operaciones que potencialmente constituyen un riesgo mayor para el derecho a la autodeterminación informativa. Se trata de la transmisión de datos, es decir, de las manipulaciones a través de las cuales los datos de carácter personal salen del ámbito en el que se estaban tratando para incorporarse a otro distinto. Se está haciendo referencia a la cesión de datos, el deber de secreto, el *outsourcing* y el movimiento internacional de datos.

I. LA CESIÓN DE DATOS.

I.1. Una visión general de la cesión.

Como se ha visto al inicio de este trabajo, las nuevas tecnologías de la información y la comunicación se han integrado en prácticamente todos los ámbitos de la vida[1910]. Estos instrumentos hacen posible una manipulación más ágil de los datos. Entre otras operaciones, las cesiones son más fáciles de llevar a cabo[1911].

Esta circunstancia puede observarse en el ámbito estrictamente social, en las tan conocidas redes sociales, en las que el flujo de información es constante. Mucho se ha escrito en los últimos años sobre las bondades y riesgos que plantean estas plazas virtuales[1912]. En todo caso, es indiscutible que a través de estas herramientas multitud de opiniones e informaciones en todos los formatos se transmiten por el globo a velocidad vertiginosa.

En lo que concierne a la Administración pública estos nuevos instrumentos redundan en una mejor realización de las tareas que le corresponden[1913]. La eficacia en el funcionamiento de la que hoy se llama Administración electrónica exige que los datos de los ciudadanos se transmitan con rapidez entre sus diferentes órganos y entre las distintas administraciones[1914]. En concreto, en el sector sanitario la necesidad de una ágil cesión de los datos de los pacientes es absoluta. Sobre todo en determinados supuestos, como los de urgencia, la posibilidad de transmitir unos datos de un lugar a otro con rapidez resulta imprescindible para la salvaguarda efectiva de la salud. Hoy día la incorporación a estos ámbitos de nuevas herramientas que hacen posible este

[1910] AIBAR y URGELL, *Estado, Burocracia…,* cit., 2007, p. 23.
[1911] MARTÍNEZ MARTÍNEZ, *Una aproximación…,* cit., 2004, p. 45.
[1912] *Report and Guidance on Privacy in Social Network Services* ("Memorándum de Roma"), adoptado por el Grupo Internacional de Trabajo en la Protección de Datos en el ámbito de las Telecomunicaciones en marzo de 2008. Revista de la APDCM *Datospersonales.org*, nº 43, 2010, dedicado a esta cuestión; VELA SÁNCHEZ MERLO, "La Privacidad…", cit., 2008, pp. 231-271; RALLO LOMBARTE y MARTÍNEZ MARTÍNEZ (Coord.), *Derecho y Redes…,* cit., 2010; CAMPUZANO TOMÉ, "Las redes sociales…", cit., 2011, pp. 29 y siguientes. "Las autoridades de Protección de Datos de más de 37 países alertan sobre la indiscreción de las redes sociales"*, El País*, 24 de octubre de 2008.
[1913] TRONCOSO REIGADA, *e-PRODAT: Administración…,* cit., 2006, pp. 8-11; GALVÁN RUIZ y GARCÍA LÓPEZ, *La Administración electrónica…,* cit., 2007, p. 25; CERRILLO i MARTÍNEZ, *Administración electrónica…,* cit., 2007, p. 17; AIBAR y URGELL, *Estado, Burocracia…,* cit., 2007, p. 28; CIERCO SEIRA, "Algunas reflexiones…", cit., 2008, p. 2.
[1914] GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración electrónica…,* cit., 2008, p. 16; VALERO TORRIJOS, "Acceso a los servicios…", cit., 2008, p. 268.

flujo de información es incuestionable. Instrumentos como la ya citada historia clínica electrónica son conocidos[1915].

Ante la evidente y masiva utilización de las TIC en todos los ámbitos de la realidad, el ordenamiento ha tenido que entrar a regular las nuevas situaciones y los nuevos problemas que se plantean con el uso de estas herramientas[1916]. El Derecho ha actuado fundamentalmente en dos direcciones. A) En primer lugar, las leyes más recientes se han hecho eco de situaciones o escenarios en que las cesiones de datos de carácter personal son necesarias. Se puede decir que las normas, conscientes de las nuevas posibilidades que plantean las TIC, se han dedicado a reconocer realidades en las que son constantes los flujos de información. De esta forma, el Derecho refleja la necesidad de incorporar las nuevas tecnologías a las distintas esferas de la vida.

En las más recientes normas que regulan la materia que aquí se trata se refleja con claridad la tendencia a asumir el hecho de que el uso de las nuevas tecnologías se va a convertir en medio indispensable de trabajo. Evidentemente este uso tendrá como resultado una mayor posibilidad de que en estos sectores las transmisiones de datos sean constantes. Se pueden citar como ejemplo dos normas que se hacen eco de esta situación. Por un lado, la reciente Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos reconoce de manera expresa en multitud de disposiciones situaciones que requieren de la transmisión de datos entre las administraciones o éstas y los ciudadanos[1917]. Sin duda alguna esta norma viene a dar un paso más con respecto a la LPAC en lo relacionado con el uso de las nuevas tecnologías por parte de la Administración[1918]. Por otro, en lo que concierne a la Administración sanitaria, la LBAP parece reconocer la necesidad de implantar la que se viene en llamar historia clínica compartida[1919]. Se trata de que en cualquier punto del Estado pueda tenerse acceso a determinados datos sanitarios de los pacientes. Este instrumento requiere necesariamente de la transmisión constante de dicha información.

[1915] CARNICERO GIMÉNEZ DE AZCÁRATE, "La historia…", cit., 2004, p. 287.

[1916] CERRILLO i MARTÍNEZ, *Administración electrónica…,* cit., 2007, pp. 18-25.

[1917] Artículo 9 LAE: "*1. Para un eficaz ejercicio del derecho reconocido en el apartado 6.2.b, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder y se encuentren en soporte electrónico, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad, de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.*

2. La disponibilidad de tales datos estará limitada estrictamente a aquellos que son requeridos a los ciudadanos por las restantes Administraciones para la tramitación y resolución de los procedimientos y actuaciones de su competencia de acuerdo con la normativa reguladora de los mismos. El acceso a los datos de carácter personal estará, además, condicionado al cumplimiento de las condiciones establecidas en el artículo 6.2.b de la presente Ley". GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración electrónica…,* cit., 2008.

[1918] GAMERO CASADO, "El Derecho Administrativo…", cit., 2008, p. 56.

[1919] DA tercera LBAP: "*Coordinación de las historias clínicas: El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición*."

B) En segundo lugar, si bien es verdad que hoy día se ha asumido la necesidad de integrar, emplear y regular las nuevas tecnologías para desarrollar diferentes aspectos de la vida y el hecho de que la información fluye, principalmente por la red, a velocidad vertiginosa, el Derecho no se ha olvidado de que la posibilidad de que las cesiones de datos se multipliquen conlleva un riesgo importante[1920].

La cesión supone que unos datos de carácter personal salen de la inicial esfera de control de su titular, quien los había transmitido directamente a otra persona, para incorporarse a otro ámbito en el que actúa un tercer sujeto ajeno a la relación entre el titular de los datos y el primer responsable del fichero[1921]. Inevitablemente, en la medida en que la información sale de esa inicial relación entre el titular y el primer responsable, en la que la posibilidad de controlar lo que sucede con los datos es más cercana, mayor es el riesgo de que éstos puedan ser empleados de forma irregular y desconocida para el titular. Cuantas más cesiones se den más lejana será la facultad de fiscalizar lo que ocurre con la información y mayor el peligro de que se pierda, de que sea sustraída, alterada, borrada o puesta en común con otros datos relativos a la misma persona[1922].

Ante la necesidad de la sociedad actual de recabar y manipular cantidades ingentes de información, no es fácil plantear una regulación especialmente limitativa de la posibilidad de llevar a cabo cesiones de datos[1923]. No obstante, la ya derogada LORTAD se hacía eco expresamente de la importancia de regular esta operación debido al peligro que conlleva. Se ponía de manifiesto en aquella norma el hecho de que la transmisión de datos facilita el cruce de información contenida en distintas fuentes, con lo cual resulta más sencillo realizar perfiles completos de las personas[1924]. Evidentemente, la cesión de datos posibilita que la información sobre una persona proveniente de diferentes fuentes converja en un único fichero, del que se pueda deducir una visión general de sus características, cualidades y gustos o preferencias.

La posibilidad de que unos datos que están siendo tratados en un ámbito determinado sean trasladados a otro, en el que una tercera persona pueda acceder a ellos y manipularlos con una finalidad que será distinta, y la posibilidad de que dicha información sea puesta en relación con

[1920] TRONCOSO REIGADA, *e-PRODAT: Administración…,* cit., 2006, p. 21; ACOSTA GALLO, "Administración electrónica…", cit., 2007, p. 3; BUISÁN GARCÍA, "Comunicación de datos ...", cit., 2008, p. 294.

[1921] SSAN, 22 de septiembre de 2004, FJ 3; 28 de noviembre 2002, FJ 3, en la que se apunta que "Al regularse la cesión de datos a terceros, el legislador tiene en cuenta el riesgo potencialmente mayor de uso indebido de los datos. En efecto, los datos salen del contexto en el cual han sido recogidos y registrados en el fichero, pasando a otro que puede obedecer a unos fines distintos. De forma tal que el dato situado dentro de un contexto y finalidad distinta permite la obtención de información del afectado o interesado distinta a aquella para la que consintió el tratamiento. La técnica denominada "data moving" o de interconexión de ficheros con fines de auditoría es un claro ejemplo del riesgo inherente a la cesión de datos". HEREDERO HIGUERAS, *La Ley...*, cit., 1996, p. 117; HERRÁN ORTIZ, *El Derecho…,* cit., 2002, p. 232.

[1922] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 86; DAVARA RODRÍGUEZ, *Guía Práctica…,* cit., 2006, p. 81.

[1923] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 46.

[1924] Exposición de Motivos LORTAD: "*(…) resulta esencial la correcta regulación de la cesión de los datos almacenados. Es, en efecto, el cruce de los datos almacenados en diversas instancias o ficheros el que puede arrojar el repetidamente aludido perfil personal, cuya obtención transgrediría los límites de la privacidad"*. DRUMMOND, *Internet, Privacidad…,* cit., 2004, p. 50, señala el riesgo de que una puesta en común de diferentes datos puede llevar a trazar un perfil completo de una persona.

otros datos que este tercero pueda ya poseer, hace que sea necesaria toda la cautela posible a la hora de llevar a cabo esta operación. La cesión requiere de todas las garantías para que se desarrolle de forma respetuosa con los derechos fundamentales, más ahora que las TIC hacen posible que los destinatarios de la información y la velocidad de la transmisión se multipliquen[1925]. Si la cesión, por sí misma, constituye un riesgo importante para la vulneración del derecho a la autodeterminación informativa, el empleo de la telemática para llevarla a cabo multiplica este peligro.

Es necesario encontrar el equilibrio entre la necesidad de un flujo ágil de información y el requerimiento de respetar el derecho a la autodeterminación informativa. Mucho más en campos como el sanitario donde los datos que se manipulan exigen, en la mayoría de los casos, cuando menos de inicio, de una especial protección[1926]. Como se verá, diferentes normas, principalmente la LOPD y la LBAP, tratan de dar solución a la colisión de bienes jurídicos que se acaba de plantear.

I.2. El régimen jurídico aplicable a las cesiones de datos sanitarios.

I.2.1. Referencia a las disposiciones que regulan la cesión en la LOPD.

El legislador, más allá de regular y plantear nuevas realidades en las que se crean tareas y funciones que requieren de la cesión de datos, consciente de la magnitud del riesgo que plantea esta operación, ha tratado de regular la comunicación de tal forma que los derechos de los ciudadanos queden salvaguardados. Esta última, es la perspectiva que aquí más interesa.

La LOPD, al contrario de la Directiva europea que ni siquiera entra a definir esta figura[1927], dedica uno de sus apartados a la cesión. Lo hace, además, en el título dirigido a regular los principios de la protección de datos. Esta Ley de integra de inicio esta figura en el concepto amplio de tratamiento[1928], como una operación más. No obstante, más adelante realiza una regulación particularizada de la cesión. Sin duda alguna, el hecho de que la norma ponga especial interés en la normación de la comunicación y el que ésta sea calificada como principio del régimen jurídico de la protección de datos pone de manifiesto la importancia de la institución que se analiza.

La regulación de la cesión viene recogida fundamentalmente en el artículo 11 de la Ley, que merece la pena reproducir a pesar de su extensión: "*Comunicación de datos.-1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.*

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

[1925] HERRÁN ORTIZ, *La Violación...*, cit., 1999, p. 258.
[1926] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 14.
[1927] GUICHOT, *Datos Personales…,* cit., 2005, p. 326.
[1928] Artículo 3.c) LOPD.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tienen atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.

4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.

5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.

6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."

A esta regulación general de la cesión se le irán añadiendo en la Ley diferentes matices dependiendo del tipo de operación que se trate. Con respecto a los ficheros públicos se encontrará una regulación específica[1929]. Lo mismo ocurre cuando se trata de ficheros privados[1930]. Para los casos en que la manipulación se lleve a cabo por las Fuerzas y Cuerpos de Seguridad la norma estatal también recoge un régimen particular[1931]. En relación a los datos concernientes a la salud, origen racial o vida sexual de las personas, la Ley señala que sólo cabrá la cesión si así lo consiente el titular de los datos o lo dispone una ley[1932]. A estos

[1929] Artículo 21 LOPD.
[1930] Artículo 27 LOPD.
[1931] Artículo 22.3 LOPD.
[1932] Artículo 7.3 LOPD.

supuestos se les podrían sumar los casos en que las cesiones de estos datos se producen con el fin de proteger la salud de las personas[1933]. Por su parte, en el apartado que regula el tratamiento de los datos sanitarios manipulados en las instituciones y centros sanitarios, al referirse a la cesión la LOPD realiza una remisión al citado artículo 11 de la Ley[1934].

Como se puede observar son numerosas las referencias que se hacen en la Ley estatal a la figura de la cesión. A la regulación expuesta se le pueden realizar numerosas críticas. Si bien se puede aceptar que debido a la complejidad de la figura no era fácil llevar a cabo una regulación especialmente precisa de la cesión, lo cierto es que la dispersión en los artículos no ayuda a expresar una valoración positiva de la Ley en este aspecto, pues en ocasiones lleva a situaciones en que se desconoce el régimen a aplicar en determinados supuestos. La norma es confusa y poco precisa. Se ha llegado a decir que es especialmente caótica, lo que redunda en detrimento de la seguridad jurídica y la claridad[1935]. A esto se irán sumando otros hechos, como son el uso continuo de conceptos especialmente ambiguos y el silencio en relación a algunos puntos fundamentales, como el relativo al ejercicio del derecho a la información en la cesión de datos, que fortalecen la crítica negativa de la regulación que se da en la LOPD a la figura de la cesión.

I.2.2. Una interpretación sobre cuál ha de ser el régimen jurídico a aplicar a las cesiones de los datos sanitarios.

Uno de los puntos conflictivos en relación a la cesión de datos se encuentra a la hora de interpretar el régimen que se ha de aplicar a la comunicación de los datos especialmente protegidos, de los datos sanitarios en particular. La LOPD recoge diferentes preceptos en los que regula la figura de la cesión, que podrían aplicarse en principio a los datos de salud. El artículo 11 regula el régimen general de las cesiones. El artículo 8, que se refiere a los datos de salud tratados en el ámbito estrictamente sanitario, en lo que toca a la cesión, realiza una remisión a dicho artículo 11. Y por su parte, el artículo 7, que concierne entre otros a los datos de salud, dispone un régimen jurídico específico que restringe la posibilidad de comunicar este tipo de datos a supuestos muy concretos. Por si esto fuera poco, en lo referente a la transmisión de datos sanitarios la LBAP recoge, tras realizar una remisión a la LOPD, una regulación concreta de la cesión de este tipo de información a determinados cesionarios[1936]. Se puede observar que

[1933] Artículo 7.6 LOPD.
[1934] Artículo 8 LOPD.
[1935] GUICHOT, *Datos Personales…,* cit., 2005, pp. 326-327.
[1936] Artículo 16 LBAP: *"3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.*
4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.
5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad

no es tarea sencilla interpretar qué preceptos serán de aplicación a la comunicación de los datos sanitarios. Esta dificultad se agranda por las continuas remisiones que se realizan entre normas y preceptos. Teniendo en cuenta que serán la LOPD y la LBAP las normas a tener en cuenta a la hora de regular la cesión de datos sanitarios, cabe preguntarse qué disposiciones de dichas leyes se aplican a las cesiones de los datos sanitarios y cómo ha de interpretarse la relación entre ellas. A pesar de su relevancia, la jurisprudencia y la doctrina se han pronunciado en pocas ocasiones sobre este interrogante.

Para aclarar esta cuestión hay que tener en cuenta diferentes puntos. A) En primer lugar, debe determinarse qué preceptos de la LOPD se aplican a las cesiones de los datos sanitarios y cómo se aplica su contenido a dichas operaciones. En la Ley, tanto el artículo 7.3 como el 8 se refieren a los datos de salud. Como se ha visto, ambos entran a regular la manipulación de este tipo de información, refiriéndose expresamente a la cesión. Cabe preguntarse, por lo tanto, cuál de ellos ha de aplicarse a la hora de regular la comunicación de los datos estrictamente sanitarios, esto es, a la comunicación de la información manipulada en el sector sanitario. La respuesta a esta cuestión ya se dio en el capítulo anterior: a pesar de que ambos preceptos se refieren a los datos de salud, regulan supuestos diferentes. Se expuso que la Ley distingue entre los datos relativos a la salud manipulados en el ámbito sanitario, recogidos en el artículo 8, que se refiere expresamente al uso de esta información en los centros e instituciones sanitarias, y los datos relativos a la salud tratados fuera de dicho ámbito, regulados en el artículo 7.3. Más allá del interés que suscita el análisis del régimen jurídico que ha de guiar la cesión de estos últimos[1937], al estar analizando aquí, exclusivamente, los problemas que plantea la manipulación de los datos sanitarios, deberá tenerse en cuenta lo dispuesto en el artículo 8, que es el que concierne a estos supuestos.

Teniendo en cuenta que ha de partirse de este precepto, hay que atender a su contenido para determinar el régimen jurídico que se ha de aplicar a las cesiones de los datos sanitarios. Se decía al analizar el derecho a consentir que el artículo 8 de la Ley lleva a cabo una normación que genera cierta confusión. Al regular el tratamiento de los datos de salud en los centros e instituciones sanitarias realiza una remisión a la normativa sanitaria. El tratamiento de los datos sanitarios deberá tomar en consideración y respetar la citada normativa. Sin embargo, salva de esta remisión la regulación concerniente a la cesión de este tipo de información. Dichas cesiones deberán tener en cuenta el artículo 11 de la LOPD. Podría interpretarse que a la hora de regular la cesión de los datos sanitarios sólo se aplicará dicho artículo 11 y no la normativa sanitaria,

de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria".

[1937] El artículo 7.3 LOPD limita los supuestos de cesión de los datos de salud a los casos en que así lo consienta el titular de los datos o lo permita una Ley por razones de interés general. Sin embargo, se plantea la posibilidad de que se incluyan más supuestos en aplicación del artículo 11.2.f), que reconoce que los datos de salud son también transmisibles en situaciones de urgencia o para realizar un estudio epidemiológico de acuerdo a lo que dicta la normativa sanitaria, o del 7.6, que permite la manipulación de los datos de salud si la finalidad es la prevención o la realización de diagnósticos médicos, la prestación de asistencia sanitaria o la gestión de servicios sanitarios o la salvaguarda del interés vital de las personas. Parece coherente interpretar que esta misma finalidad, al igual que justifica un tratamiento ordinario, puede justificar la cesión de este tipo de datos, a pesar de que dicha comunicación no esté prevista en el apartado de la Ley que regula la protección de los datos de salud, sino en la sección que afecta a los datos comunes. MESSÍA de la CERDA BALLESTEROS, *La cesión o comunicación…*, cit., 2003, p. 299; NICOLÁS JIMÉNEZ, *La protección jurídica…,* cit., 2006, p. 210.

entre la que se encuentra la LBAP, pues así lo dispone expresamente el artículo 8 de la LOPD al excluir de la remisión a la normativa sanitaria la regulación de la cesión.

No parece que esta conclusión sea acertada. Si bien es cierto que el artículo 8 salva de la remisión a la normativa sanitaria la regulación de la cesión de los datos sanitarios, no parece que pueda interpretarse que, debido a esta disposición, la LBAP queda inaplicada en este punto. Hay que valorar que esta Ley, a pesar de realizar también una remisión general a la LOPD, regula por sí misma el régimen de la cesión de datos sanitarios. No tiene lógica que se interprete que esta regulación no tiene aplicación. Lo cierto es que cuando se aprobó la LOPD todavía no había entrado en vigor la LBAP y se carecía de una regulación aplicable a este tipo de operaciones. Hoy día, con una normativa sanitaria más completa, ha de interpretarse la remisión que el artículo 8 de la Ley estatal de protección de datos realiza a la normativa sanitaria como una remisión genérica, de manera que afecte también a la regulación de las cesiones. De esta forma, más allá del citado artículo 11 deberán tenerse en cuenta las normas que regulan el sector de la salud. Se puede concluir, por lo tanto, que el régimen jurídico a aplicar a las cesiones de los datos sanitarios vendrá de la interpretación conjunta de la normativa de protección de datos y la normativa sanitaria. Las remisiones mutuas que se hacen la LOPD y la LBAP avalan este criterio. Ante la confusión que genera el entramado normativo que entra a regular las cesiones de los datos sanitarios, cierta claridad debe llegar de esta interpretación conjunta.

La relación entre el artículo 8 y 11 de la LOPD ha de reinterpretarse a la luz de la normativa sanitaria. Esta reinterpretación ha de comenzar con la revisión del alcance de la remisión que realiza el primero de los preceptos al segundo. El artículo 8 se remite al artículo 11 de la misma Ley, que, no hay que olvidar, fija el régimen jurídico general referente a la cesión de los datos de carácter personal. Dicha remisión es genérica, sin matiz alguno, a todo el artículo 11, de forma que podría parecer que la regulación contenida en este último precepto es aplicable también al supuesto de hecho recogido en el artículo 8[1938]. El artículo 11, por un lado, regula los requisitos que se han de cumplir para poder comunicar los datos de carácter personal a terceras personas, fundamentalmente, la necesidad de requerir el consentimiento del titular de los datos. Por otro, fija una serie de supuestos en que dicho consentimiento no es necesario. Hay que preguntarse si este contenido es de aplicación en toda su extensión para las comunicaciones de los datos sanitarios.

Para responder a esta cuestión ha de partirse de la siguiente premisa: el artículo 11 regula el régimen general de las cesiones, aplicable a los datos comunes. Sin embargo, los datos de salud

[1938] MURILLO DE LA CUEVA, "El derecho…", cit., 2006, p. 35: "La posibilidad de que terceros no vinculados por relaciones de parentesco, legales o de hecho, accedan a los datos relativos a la salud de una persona existe solamente en las hipótesis expresamente contempladas por las leyes. Es decir, en aquellas en las que cabe la cesión o comunicación de los datos de acuerdo con el artículo 11 de la LOPD y con el artículo 16 de la Ley 41/2000";SANZ CALVO, "Datos relativos…", cit., 2008, pp. 239-240: "Aunque la redacción no es especialmente clara, parece deducirse que, con independencia de lo que se refleja en el precepto y que luego se analiza, resulta aplicable lo dispuesto en el artículo 11". Artículo 67.2 Ley 17/2010, 8 de noviembre, de Derechos y Deberes de las Personas en Materia de Salud en la Comunidad Foral de Navarra, en el que se permite el acceso a la historia clínica de un paciente, sin necesidad de su consentimiento, en los casos previstos en los artículos 11.2 y 22 LOPD. La remisión a estos preceptos es genérica, sin matiz alguno: "*Se exceptúa de lo previsto en el apartado anterior el acceso a la historia clínica en los supuestos previstos en los artículos 11.2 y 22 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal*".

son considerados por la Ley no como datos comunes, sino como merecedores de una protección especial. Se entiende aquí que es necesario realizar una interpretación sistemática de la LOPD para extraer una conclusión[1939]. Cuando se analizó la figura del consentimiento se concluyó que la Ley reconocía un régimen específico para los datos especialmente protegidos[1940], distinto al sistema fijado para los datos comunes[1941], y se señaló que la regulación del consentimiento para los primeros era más exigente, requiriéndose mayores garantías para que fuera válido. Estas mayores garantías se aplicaban, sobre todo, a la hora de exceptuar el consentimiento para manipular los datos de carácter personal. Los supuestos en que se podía limitar este derecho eran menos cuando se trataba de datos especialmente protegidos.

Se entiende aquí que empleando el mismo criterio que utiliza la LOPD a la hora de regular el consentimiento, que diferencia entre el régimen general y el régimen especial dedicado a este tipo de datos llamados sensibles, no puede aplicarse dicho sistema general, dirigido a los datos comunes, a la cesión a los datos sanitarios sin realizar ninguna matización[1942]. La regulación específica, referida a los datos sensibles, desplazaría a la general concerniente a los datos comunes[1943]. La jurisprudencia en algún caso se ha hecho eco de esta consideración al señalar, en aplicación del artículo 7.3 de la Ley, que las excepciones al consentimiento en la cesión de datos de salud deben limitarse a los supuestos en que así lo disponga una Ley e interpretarse en sentido restrictivo[1944]. Así, los requisitos para que la cesión de estos datos sensibles sea válida y, sobre todo, las excepciones a la necesidad de requerir el consentimiento para llevarla a cabo deberían determinarse, no realizando una remisión sin matices al contenido completo del artículo 11, sino aplicando un sistema específico configurado para los datos necesitados de una especial protección[1945].

El problema reside en que no hay una regulación lo suficientemente clara y desarrollada dirigida a concretar cómo se han de realizar las cesiones de este tipo de datos. Hubiera sido preferible que el propio artículo 8 entrara a regular por sí mismo esta materia, pues se hubiera ganado en claridad. Sin embargo, frente a esto, el punto de partida que presenta el citado precepto a la hora de definir el régimen jurídico a seguir en las cesiones de los datos sanitarios lo constituye una remisión al artículo 11 de la Ley, que ha de ser interpretada de manera restrictiva, y una remisión general, de la que se salva la figura de la cesión, a la normativa sanitaria. Una normativa, ésta última, que, además, contiene, por su parte, una regulación propia de la cesión de datos sanitarios.

B) En segundo lugar, tras determinar el alcance de la remisión al artículo 11, es necesario fijar los criterios por los que se determina el régimen jurídico a aplicar en la regulación de las cesiones de los datos sanitarios. Como se ha dicho, la solución ha de venir de la interpretación conjunta entre la normativa sanitaria y la referente a la protección de datos.

[1939] NICOLÁS JIMÉNEZ, *La Protección…,* cit., 2006, p. 210.
[1940] Regulado en el artículo 7 LOPD.
[1941] Regulado en el artículo 6 LOPD.
[1942] TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 999.
[1943] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 85.
[1944] SAN 31 de enero de 2008, FJ 3.
[1945] Informe jurídico de la AEPD "Cesión de datos de salud para fines de investigación", 0509/2009.

En relación a los requisitos que se han de cumplir para ceder los datos sanitarios hay que tener en cuenta, primero, lo dispuesto en el artículo 11 de la LOPD. Sin embargo, como se irá viendo, estos requisitos serán matizados. Por ejemplo, si bien el régimen general exige el consentimiento, se entiende que sencillo, cuando se trata de datos de salud ese consentimiento deberá ser expreso. Esta regulación contenida en la normativa de protección de datos deberá ser matizada en atención a lo que fija para determinados casos la normativa sanitaria.

En relación a las excepciones la interpretación habrá de ser especialmente restrictiva. La remisión del artículo 8 de la LOPD al 11 no ha de interpretarse como una remisión general. Hay que realizar una lectura restrictiva de este último precepto. Antes se ha dicho que el hecho de que la LOPD aplicara un régimen jurídico especial o diferenciado a los datos sensible, cuando se trataba de regular el consentimiento, constituía indicio suficiente para afirmar que esta misma diferenciación debe hacerse también cuando lo regulado era la cesión de este tipo de datos sensibles. Si las excepciones a aplicar al derecho a consentir el tratamiento son menos cuando se trata de datos especialmente protegidos, caso de los de salud, parece adecuado pensar que lo mismo ocurrirá cuando se trate de limitar el derecho a autorizar la cesión de este tipo de información. Esta idea se refuerza por el hecho de que muchas de las excepciones que se recogen en el artículo 6 de la Ley, referido al consentimiento en el tratamiento de los datos comunes, se reproducen en el artículo 11, en la regulación del consentimiento en la cesión de datos. La mayoría de las excepciones del artículo 6 se aplican al consentimiento cuando se trata de datos comunes, pero no a los datos especialmente protegidos, que se rigen por un régimen particular. Pues bien, esas mismas excepciones se recogen, en algunos casos, también en el artículo 11. Por lo tanto, cabe preguntarse si son aplicables a los datos objeto de una especial protección. Lógicamente, si se entendía que estas excepciones no se podían aplicar al consentimiento, cuando se trataba de datos referentes a la salud, parece coherente interpretar que estas mismas excepciones que no se podían aplicar entonces no serán aplicables a la cesión de estos datos. Es lo que ocurre, por ejemplo, con la excepción concerniente al tratamiento de datos considerado necesario para el mantenimiento o cumplimiento de una relación negocial, laboral o administrativa, que se encontraba en el artículo 6 de la Ley, regulador del consentimiento, y que también se recoge en el artículo 11, regulador de la cesión. Esta excepción no se aplicaba al consentimiento para el tratamiento de datos de salud, pues la regulación de este tipo de datos se rige por un régimen propio. Por lo tanto, parece lógico pensar que esta excepción que no se aplicaba entonces tampoco se aplicará a la cesión de este tipo de información.

A la hora de regular las excepciones al consentimiento en la cesión de datos sanitarios habrá que realizar también una interpretación conjunta de la normativa de protección de datos y la sanitaria. El artículo 11 de la LOPD reconoce casos concretos dirigidos específicamente a los datos de salud. Dispone, por ejemplo, en uno de sus apartados que no será necesaria la autorización del titular de los datos relativos a la salud, cuando dicha cesión sea necesaria para solucionar una situación de urgencia o para desarrollar investigaciones epidemiológicas de acuerdo con la legislación sanitaria estatal o autonómica[1946]. Parece evidente que este supuesto

[1946] Artículo 11.2.f) LOPD.

tiene aplicación en el ámbito sanitario. Sin embargo, los demás casos recogidos en la citada disposición podrían plantear dudas[1947]. Hay que tener en cuenta además que en el articulado de la LOPD se reconocen más preceptos que posibilitan una cesión sin consentimiento del titular. Es el caso en que los datos son empleados por las administraciones[1948] o, más concretamente, por las Fuerzas y Cuerpos de Seguridad[1949]. Para interpretar la aplicabilidad de todas estas excepciones a las cesiones de los datos sanitarios será necesario realizar una interpretación conjunta entre la LOPD y la LBAP.

Más adelante se analizarán las excepciones por separado. Baste ahora con subrayar, que el articulado de la LOPD ha de interpretarse en sentido restrictivo, y que no todos los límites al consentimiento dispuestos en el mismo serán aplicables a las comunicaciones de los datos sanitarios. Además, será necesario que a la hora de interpretar estos límites se tenga en cuenta la normativa sanitaria.

I.3. Concepto.

Para poder realizar un análisis medianamente riguroso del régimen jurídico que establecen las normas sobre la cesión de datos sanitarios, será necesario antes de nada aclarar a qué se hace referencia cuando se habla de la cesión. Con este fin, se acudirá primero al texto de la LOPD, para aportar después una definición más concreta del concepto de cesión partiendo de la realidad sanitaria.

I.3.1. El concepto de cesión en la LOPD.

I.3.1.A. El concepto de cesión en las normas. Acercamiento a una interpretación amplia desde la normativa penal.

Diferentes normas han dado distintas definiciones de la figura que ahora se trata. La anterior Ley reguladora del tratamiento automatizado de los datos de carácter personal no daba una definición de la cesión. La actual LOPD define la cesión o comunicación de datos como "*toda revelación de datos realizada a una persona distinta del interesado*"[1950]. En la misma línea el vigente reglamento de desarrollo de la Ley entiende por cesión o comunicación el "*tratamiento de datos que supone su revelación a una persona distinta del interesado*"[1951]. El anterior reglamento definía la cesión como "*toda obtención de datos resultante de la consulta de un fichero, la publicación de los datos contenidos en el fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada*"[1952]. La Directiva europea no recoge una definición expresa del término cesión, pero de la aclaración que realiza

[1947] VALERO TORRIJOS, *Comentarios a la Ley...,* cit., 2001, p. 136: parece entender que en relación a las cesiones de datos de salud se aplica la excepción del artículo 11.2.f), pero que, sin embargo, para los demás casos será necesario el consentimiento del titular; TRONCOSO REIGADA, *Protección de Datos*…, cit., 2008, p. 85.
[1948] Artículo 21 LOPD.
[1949] Artículo 22.3 LOPD.
[1950] Artículo 3.i LOPD.
[1951] Artículo 5.1.c) RDLOPD.
[1952] Artículo 1.2 RD 1332/1994, de 20 de junio, 20 de junio de 2004, por el que se Desarrollan Algunos Puntos de la LORTAD.

del concepto de tratamiento se desprende que la cesión es "*comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión"*[1953]*.* Además, la norma europea da contenido a los conceptos de tercero, "*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento de del encargado del tratamiento"* y destinatario, *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios*". La Recomendación del Consejo de Europa sobre el tratamiento de los datos médicos tampoco da una definición de este concepto, pero interesa apuntar que cuando regula la cesión de los datos habla de "comunicación", lo cual, como luego se verá, sugiere una acepción amplia del concepto. Otras recomendaciones del mismo organismo han definido la comunicación como "*el acto de hacer los datos personales accesibles a terceras personas, independientemente del medio o soporte empleado"*[1954] o como "*hacer los ficheros y datos personales accesibles, autorizando su consulta, transmitiéndolos o diseminándolos, o haciéndolos disponibles, independientemente del medio o soporte empleado"*[1955]*.*

La necesidad de dar una definición al concepto de cesión se ha observado en normas distintas a las referidas a la materia de protección de datos. En el ámbito penal, en los tipos concernientes a los delitos de descubrimiento y revelación de secretos[1956], se recogen diferentes verbos cuyo contenido no es sencillo de determinar, a saber: divulgar, revelar, ceder, difundir, son utilizados indistintamente. La doctrina ha tratado de dar un sentido concreto a estos conceptos[1957]. Lo cierto es que no resulta fácil delimitar con precisión los contornos de los

[1953] Artículo 2.b) Directiva 95/46/CE.

[1954] Punto 1 Recomendación nº 18 (97) del Consejo de Europa relativa a la Protección de Datos Personales Recogidos y Procesados con Fines Estadísticos*: "Communication refers to the act of making personal data accessible to third parties, regardless of the means or media used".*

[1955] Punto 1 Recomendación 10 (91) relativa a la Comunicación a Terceros de los Datos en poder de los Organismos Públicos*:* "*The expression "communication" refers to making files or personal data accessible, such as by authorising their consultation, transmitting them, disseminating them or making them available regardless of the means or media used".*

[1956] Artículo 197 y siguientes CP.

[1957] GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 315: en relación al 197.3 CP; "La difusión parece referirse a hacer del dominio público datos de carácter personal que tienen la consideración de *reservados. Difundir* es dar a conocer, extender a una colectividad indeterminada los secretos a los que ha accedido el autor, divulgándolos públicamente (…)".

"La *revelación* requiere que lo que era secreto o pertenecía al ámbito reservado de la intimidad se comunique a otra persona y equivale a descubrir o manifestar lo desconocido o secreto, esto es, a poner en conocimiento de otro lo que el sujeto ha descubierto por sí"; GÓMEZ RIVERO, *La Protección…,* cit., 2007, p. 159: "Las dudas interpretativas en torno a cuál sea la dimensión de la conducta de divulgar a efectos del art. 199.2 vienen propiciadas por el hecho de que, si bien está claro que con ella el legislador apunta a la comunicación de los datos a terceros, utiliza una expresión distinta de la que emplea tanto en el art. 197 como en el apartado precedente (…). Así, mientras en el art. 197.3 emplea los verbos <<*difunden, revelen o ceden*>>, y en el art. 199.1 castiga al que <<*revelare*>> secretos ajenos, en el apartado que aquí interesa utiliza el término <<*divulgar*>> (…)".

p. 171: "deben quedar fuera del ámbito típico de la rt. 199.2 todos los casos en que, no ya el destinatario concreto, sino en general cualquier persona hubiera podido tener acceso a la información por tratarse de hechos *cognoscibles* por cualquiera, bien sea en el presente o bien en el futuro inmediato".

p. 316: "*Ceder a terceros* es transmitir a otro/s el objeto de conocimiento al que ha accedido el autor. Por <<ceder>> ha de entenderse transferir información".

mismos, pues la mayoría de las veces cuentan con un contenido muy parecido, cuando no idéntico, como puede desprenderse de sus definiciones[1958]. En todo caso, el que la normativa penal haya recogido todas estas acciones como hechos punibles podría llevar a interpretar que se quiere dar un alcance especialmente amplio a estos tipos penales, abarcando toda acción que suponga que una información que se pretende preservar dentro de una esfera de conocimiento salga fuera de ese ámbito de protección. Partiendo de esta interpretación podría pensarse, por ejemplo, que se castiga la revelación independientemente de que se pueda constatar que un sujeto extraño, un tercero concreto, ha accedido a la información o no.

La interpretación amplia de estos conceptos en el ámbito penal, sin embargo, plantea problemas. El hecho de que el Derecho penal sea considerado como *última ratio*[1959] hace difícil que se pueda realizar dicha interpretación amplia, a pesar de que la redacción de los tipos penales y el uso de todos los conceptos citados pudieran llevar a pensar lo contrario. El efecto o resultado tan grave que acarrea la aplicación del derecho penal hace que las normas que lo componen no deban ser interpretadas en sentido expansivo. Esta necesidad de interpretar las normas penales de manera restrictiva ha llevado a comprender que queda fuera del ámbito de aplicación del delito de divulgación de secretos[1960] la acción de crear o generar simplemente la posibilidad de que terceras personas puedan acceder a la información protegida por el secreto profesional. Es decir, no habría divulgación de secreto, y por lo tanto no podría aplicarse ese tipo penal concreto, si con la actuación del imputado sólo se genera o crea la posibilidad de que un tercero pueda conocer el contenido de esos secretos[1961]. Parece necesario para aplicar este tipo penal, que esa tercera persona, sea un único sujeto o varios, tenga acceso efectivo a dicha información. Más allá de que esta acción pudiera tener cabida en otro precepto[1962], es sabido que la normativa penal exige de una interpretación restrictiva.

[1958] Según la RAE, en http://www.rae.es/rae.html: revelar: "Descubrir o manifestar lo desconocido o ignorado"; divulgar: "Publicar, extender, poner al alcance del público algo"; difundir: "Extender, esparcir, propagar físicamente"; ceder: "Dar, transferir, traspasar a alguien una cosa, acción o derecho"; JORGE BARREIRO, "Delitos contra…", cit., 1997, p. 582: en relación al artículo 199.1: "La acción típica de <<*revelar*>> ha de considerarse sinónima de la de <<*divulgar*>>, es decir, ha de ser entendida como <<la comunicación a una o más personas no poseedoras del secreto>>"; MORANT VIDAL, *Protección Penal…,* cit., 2003, pp. 78-79; RUEDA MARTÍN, *Protección Penal…,* cti., 2004, pp. 96-97; MORALES PRATS, "Delitos contra la intimidad…", cit., 2009, pp. 449-450.

[1959] Exposición de Motivos CP. STC 24 de febrero de 2004, FJ 5, señala que "la sanción penal sólo resulta necesaria cuando no existen otras vías de protección alternativas en el ordenamiento jurídico menos restrictivas de derechos y suficientes para obtener la finalidad deseada (última ratio)"; STS 1 de febrero de 2007, FJ 3, por su parte, apunta que "la tipicidad es la verdadera enseña y divisa de la antijuridicidad penal, quedando extramuros de ella el resto de las ilicitudes para las que la <<sanción>> existe pero no es penal. Sólo así se salvaguarda la función del derecho penal, como última ratio y el principio de la mínima intervención que lo inspira". BACIGALUPO, *Teoría y Práctica del Derecho Penal…,* cit., 2009, p. 75.

[1960] Artículo 199.2 CP. QUERALT JIMÉNEZ, *Derecho Penal español…,* cit., 2008, p. 278.

[1961] GÓMEZ RIVERO, *La Protección…,* cit., 2007, p. 171: "deben quedar fuera del ámbito típico del art. 199.2 todos los casos en que, no ya el destinatario concreto, sino en general cualquier persona hubiera podido tener acceso a la información por tratarse de hechos *cognoscibles* por cualquiera, bien sea en el presente o bien en el futuro inmediato".

[1962] Podría aplicarse, en este sentido, el artículo 197.3 CP: "*Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior". Este precepto ha sido empleado, por ejemplo, para sancionar a un periodista por publicar datos de salud de determinados reclusos que padecían SIDA. MORALES PRATS, "Delitos contra la intimidad…", cit., 2009,

Constituye el Derecho penal un ámbito en el que la doctrina y la jurisprudencia son más exigentes y elaboran una dogmática más fina a la hora de interpretar los preceptos y términos que se utilizan en la regulación de los tipos penales. Sin embargo, fuera de este ámbito, estos términos, como ocurre con el concepto de cesión, pueden ser entendidos de otra manera. Las interpretaciones más restrictivas que se puedan dar desde el ámbito penal del concepto de cesión no tienen porqué condicionar el contenido que en este trabajo se va a exponer de dicho término.

I.3.1.B. Sobre la posibilidad de realizar una interpretación amplia del concepto cesión partiendo de la LOPD.

De una primera lectura de las definiciones que se han dado en la normativa de protección de datos podría entenderse por cesión la transmisión de unos datos por parte de una persona a otra, que se hace con ellos para llevar a cabo una finalidad concreta. Partiendo de esta interpretación se entendería que es necesario que haya un cedente y un cesionario, y que este último se haga con los datos para llevar a cabo un nuevo tratamiento[1963]. De esta forma los casos en que el tercero cesionario no accediera efectivamente a los datos para llevar a cabo una manipulación de los mismos quedarían fuera del concepto de cesión. No habría comunicación si los datos solamente salieran a la luz y simplemente se generara la posibilidad de que un tercero acceda a la información, pero sin que hubiera constancia de dicho acceso.

Sin embargo, más allá de esta acepción clásica de la cesión, se podría deducir del contenido de las normas una interpretación más amplia del concepto. Esta interpretación llevaría a entender por cesión toda revelación de datos. Según este criterio, incluso el mero hecho de que una tercera persona, ajena a la relación entre el titular de los datos y el responsable del fichero, tenga la posibilidad de acceder a los datos podría constituir una cesión[1964]. Una publicación, por ejemplo, en un tablón de anuncios de una serie de datos supondría una cesión. No haría falta por lo tanto que los datos fueran recogidos físicamente por el cesionario en un nuevo fichero para un posterior tratamiento, sino que bastaría con su difusión, con sacar los datos a la luz, para que se considerara una cesión de datos. Es más, ni siquiera sería necesario, según esta interpretación, que hubiera un destinatario determinado que llegara a captar la información, sino que sería suficiente con que cupiera la posibilidad de que personas extrañas accedieran a los datos de carácter personal para entender que existe una cesión[1965].

---

p. 435. Juzgado de Primera Instancia de Madrid, 18 de diciembre de 2009 FJ 3: "lo cierto es que se trata de una cesión universal por cuanto tiene acceso a la citada información todo el que la quiera ver, esto es, es libre", actividad que posteriormente se incluye en los tipos penales descritos en los artículos 197.2. y 3 CP.

[1963] HEREDERO HIGUERAS, *La Ley...*, cit., 1996, p. 75, ha afirmado en esta línea que la "mera visualización en pantalla sería una consulta, pero si no va acompañada de un nuevo almacenamiento no sería cesión". Señala este autor que "con la publicación de los datos de un fichero, los datos pasan a ser accesibles al público con lo cual quedan excluidos de la ley o de parte de sus preceptos, pero no son cedidos, pues no cabe una cesión sin especificar el cesionario"; GONZÁLEZ NAVARRO, "El Derecho...", cit., 1996, p. 48.

[1964] Recomendación 2/2004, de 30 de julio, de la APDCM, sobre Custodia, Archivo y Seguridad de los Datos de Carácter Personal de las Historias Clínicas no Informatizadas se aclara que el acceso por tercero, recogido en el artículo 16 de la Ley 41/2002, constituye una cesión de datos.

[1965] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...,* cit., 2003, p. 59; MESSÍA DE LA CERDA BALLESTEROS, "Consideraciones sobre la regulación…", cit., 2010, p. 1.010. STS 2 de diciembre de 2009, FJ 2, de

La asunción de esta postura resultaría muy importante en ámbitos como el sanitario, donde la mera vulneración del secreto profesional haciendo público un dato sanitario de un usuario o paciente podría constituir una cesión contraria a Derecho. Conocidos casos como la pérdida de historias clínicas o los supuestos en que se han encontrado estos documentos en la basura podrían tener cabida en este concepto[1966]. Lo mismo ocurre con los casos en que varias historias clínicas aparecen por descuido colgadas en Internet[1967]. Puede entenderse que estos supuestos no sean penalmente sancionables, pero no que no se les puedan aplicar sanciones administrativas.

De las definiciones dadas por la mayoría de las normas se podría deducir una interpretación amplia del concepto[1968]. Esta interpretación es especialmente reconocible en las recomendaciones del Consejo de Europa, donde se define la cesión como la acción de hacer los datos accesibles a terceros. Si para que haya una comunicación basta con hacer los datos accesibles a terceras personas, la mera posibilidad de que extraños accedan a la información constituirá una cesión. La Directiva europea sigue la misma interpretación al referirse a la cesión como cualquier forma que posibilite el acceso a los datos. En ningún momento se exige que la tercera persona, cesionaria, tenga que hacerse con los datos.

En la normativa estatal también se encuentran diferentes indicios que llevan a afirmar que se ha adoptado una interpretación amplia del concepto cesión. Primero, es significativo que la actual Ley, de la misma forma que lo hace el reciente reglamento que la desarrolla, emplee los términos "toda revelación" a la hora de definir la cesión de datos. La equiparación entre cesión y revelación de información deja entrever que se ha hecho eco de la interpretación amplia de la cesión. Revelar no es otra cosa sino "descubrir o manifestar lo ignorado o secreto"[1969]. Para que se pueda hablar de revelación no es necesario que los datos se transmitan a una persona concreta, por lo que bastará con que los datos simplemente salgan a la luz.

Segundo, es clarificador que en la normativa estatal se emplee el término comunicación como sinónimo de cesión. Hay que tener en cuenta que la actual LOPD cambia el enunciado del artículo 11, concerniente a la cesión, con respecto a la anterior Ley. Esta última se refería en este punto a la "cesión de datos", mientras que la Ley vigente recoge la expresión "comunicación de datos". Si bien en un primer momento este cambio puede parecer insignificante, se cree que efectivamente responde a una voluntad clara de darle un sentido amplio al concepto de cesión. Así lo ha visto también parte de la doctrina[1970]. Comunicar supone "hacer a uno partícipe de lo que uno tiene" o "descubrir, manifestar o hacer saber a alguien algo"[1971]. Descubrir, hacer público

---

la que se desprende que cuando no cabe posibilidad de que un tercero pueda acceder a los datos es imposible considerar que ha habido cesión o revelación de datos. Es lo que ocurre cuando en una nómina entregada al trabajador en sobre cerrado aparece el nombre del sindicato al que éste está afiliado. A pesar de que resulta un hecho extraño, no puede entenderse que la inclusión de esta información constituye una cesión o revelación.

[1966] "Hallados en la calle los datos de 173 trasplantados en un hospital catalán", *El país,* 3 de noviembre de 2009.

[1967] "Una negligencia lleva a la Red datos de 4.000 mujeres que abortaron", *El País*, 25 de abril de 2008.

[1968] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 158.

[1969] http://www.rae.es/rae.html. SAN 11 de febrero de 2004, FJ 3.

[1970] FREIXAS GUTIERREZ, *La Protección...*, cit., 2001, p. 155, asegura que el concepto comunicación "tiene una interpretación mucho más amplia que el de cesión, incluyendo todas aquellas actuaciones tendentes a propagar, informar o difundir los datos que se poseen"; APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 221.

[1971] http://www.rae.es/

o patente, sugiere que no es necesario que un cesionario se haga físicamente con los datos para que se entienda que hay cesión[1972].

De la comparación entre la Ley hoy vigente y la anterior LORTAD pueden sacarse otras conclusiones que favorecen la interpretación amplia. La derogada norma exigía que el consentimiento en la cesión recayera sobre un cesionario determinado o determinable[1973]. De esta manera, las transmisiones en que el cesionario era indeterminable no podían considerarse cesiones. Así ocurriría, por ejemplo, en el supuesto en que unos datos de carácter personal salen a la luz, se publican, sin un destinatario concreto. Estas acciones no se considerarían, a efectos de aplicar la LORTAD, como cesión. En la medida en que la cesión requería concretar el cesionario, la simple publicación de unos datos, que hace difícil dicha concreción, no podía considerarse como tal. La actual Ley no recoge la citada exigencia. No es necesario que el cesionario sea determinado o determinable. Esta reforma lleva a pensar que se abre una puerta para que supuestos como mera la publicación tengan cabida en el concepto de cesión. La adopción de la acepción amplia es, atendiendo a lo visto hasta ahora, posible sin tener que hacer una interpretación forzada de las normas.

La AEPD parece haberse decantado también por la interpretación amplia del concepto. Es lo que se puede deducir cuando en alguna de sus memorias concluye que la publicación de unos datos en una página *web* constituye una cesión de datos[1974] y cuando en sus resoluciones, haciéndose eco de la jurisprudencia, interpreta que por cesión ha de entenderse "toda obtención de datos resultante de la consulta de un fichero"[1975]. En diferentes informes jurídicos ha aplicado también la normativa relativa a la cesión a acciones en que los datos simplemente eran difundidos en Internet o publicados en tablones, sin que se dirigieran a cesionarios determinados[1976]. También la jurisprudencia parece haber asumido en algunas decisiones la interpretación amplia[1977]. Se ha llegado a afirmar que "dicho concepto de cesión no puede ser más amplio, pues entiende por tal toda revelación de datos realizada a una persona distinta del interesado"[1978]. Las referencias, tanto por parte de la AEPD como de los tribunales, a la cesión

[1972] NAVALPOTRO, RODRÍGUEZ y TANÚS, "Críticas a la nueva...", cit., en http://www.geocities.com/, ha criticado el hecho de que la LOPD emplee los conceptos de cesión y comunicación como si fueran sinónimos, debido a que, en realidad, no son términos equivalentes, lo cual "provoca una innecesaria confusión terminológica"; APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 120, afirma que los conceptos de cesión y comunicación "se refieren, por su significado, a dos tipos de actuación fácilmente diferenciables y que tienen pocos aspectos en común". Si bien es cierto que el uso alternativo de estos dos conceptos puede generar confusión, a nuestro entender, el que estos dos términos se empleen de manera indistinta en la norma, aclara el significado del concepto cesión otorgándole un sentido amplio. Apoyamos por lo tanto, junto a ULL PONT, *Derecho Público...*, cit., 2000, p. 129, y MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, pp. 40-41, el empleo del término "comunicación" por parte de la LOPD. APDCM, *Guía de protección…*, cit., 2004, p. 274: "La simple visualización por un tercero o la comunicación de cualquier dato al mismo, por ejemplo al realizar una consulta telefónica, constituye una cesión de datos".

[1973] Artículo 11.3 LORTAD: "*Será nulo el consentimiento cuando no recaiga sobre un cesionario determinado o determinable, o si no constase con claridad la finalidad de la cesión que se consiente*".

[1974] Memoria de la AEPD de 2002, p. 240.

[1975] Resolución AEPD, R/00063/2003, de 21 de febrero de 2003, procedimiento PS/00105/2002.

[1976] Informe jurídico AEPD, "Difusión de datos de sentencias condenatorias por negligencia médica", 2000; Informe jurídico AEPD, "Publicación de datos en procesos selectivos", 2007; Informe jurídico AEPD, 0074/2009

[1977] BUISÁN GARCÍA, "Comunicación de datos…", cit., 2008, pp. 288-289; SAN de 18 de mayo de 2006, FJ 4.

[1978] SSAN, 21 de junio de 2002, FJ. 5; 30 de junio 2004; 9 de mayo 2007; 24 de mayo 2007, FJ. 4: "Es tal cesión de datos personales, conforme a reiterada doctrina de esta Sala, un concepto jurídico de gran amplitud y así, cualquier

como “toda obtención” o “toda revelación” reflejan esta voluntad de interpretar el concepto de manera expansiva.

Es posible por lo tanto partir, en lo referente a la LOPD, de un concepto amplio de la cesión. De esta manera se otorgaría una mayor protección a los titulares de los datos, que contarían con un mayor control sobre dicha información en todo tipo de transmisiones. Esta interpretación amplia choca, sin embargo, con la regulación que hace la Ley de otra figura estrechamente vinculada con la comunicación. Se está hablando del deber de secreto que imponen las normas de protección de datos a las personas que tienen la función de manipular dicha información. Como se verá a continuación, el reconocimiento en la Ley, en un apartado distinto al de la cesión, del deber de secreto hace imposible que se pueda adoptar la citada interpretación amplia.

I.3.1.C. La cesión de datos y el deber de secreto. La necesidad de interpretar el concepto de cesión de forma restrictiva.

La definición que se ha dado del concepto de cesión ha de ponerse en relación con otra figura reconocida en la LOPD. Se está hablando del deber de secreto. Señala la Ley que el responsable del fichero o cualquier persona que intervenga en el tratamiento de los datos de carácter personal estará obligado a respetar el secreto profesional y a guardar dichos datos, incluso después de finalizar su relación con el titular de los datos o, cuando se trata de personas que trabajan para el responsable del fichero, con este último[1979]. El incumplimiento de este deber de secreto será objeto de sanción[1980]. Esta previsión ya venía recogida en la anterior LORTAD[1981] y también en la Directiva. La norma europea regula este deber de secreto en un apartado separado junto al principio de seguridad[1982]. La relación entre estos dos principios es evidente. En ambos casos se trata de asegurar que unos datos no puedan salir de la esfera de control inicial que se crea entre el titular de los datos y el responsable del fichero[1983]. El incumplimiento de las medidas de seguridad abre la puerta para que los datos puedan salir a la luz y difundirse, vulnerando así el deber de secreto[1984]. Fuera de la normativa de protección de datos el deber de secreto cuenta también, como se ha visto, con protección y reconocimiento. Así sucede en las

revelación o manifestación de datos a un tercero, distinto del interesado, constituye cesión o comunicación de los mismos a efectos de la LOPD. En el mismo sentido DEL PESO NAVARRO, *Ley de Protección...*, cit., 2000, p. 44, entiende que “la simple revelación de datos de una sola persona se considera una cesión”.

[1979] Artículo 10 LOPD: “*El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo*”.

[1980] Artículos 44.2.a), 44.3.g) y 44.4.g) LOPD. SAN 29 de septiembre de 2004: se aclara cuando el incumplimiento del deber de secreto es una infracción grave o leve.

[1981] Artículo 10 LORTAD.

[1982] Artículos 16 y 17 Directiva 95/46/CE.

[1983] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 216.

[1984] SAN 9 de julio de 2007, FJ 2: “Este Art. 10 , junto con el Art. 9 LOPD que regula las medidas de seguridad, contiene una regla que afecta a la confidencialidad como parte de la seguridad, por lo que se refiere especialmente al responsable del fichero y a las personas que hayan participado en el tratamiento”. Resolución AEPD R/00791/2010, procedimiento AP/00067/2009, 6 de abril de 2010.

normas penales[1985] y en la normativa civil[1986]. En el ámbito de la Administración las leyes imponen también la obligación de guardar sigilo a los funcionarios[1987].

El deber de secreto ha sido también una figura regulada en el ámbito sanitario. La LBAP reconoce el derecho a la intimidad de los pacientes[1988]. Esta misma norma establece la obligación de toda persona que elabore o tenga acceso a la información de guardar la debida reserva[1989]. La LGS recoge por su parte el derecho a la confidencialidad de los pacientes[1990]. El Código de Ética y Deontología Médica subraya también la obligación de los profesionales de la sanidad de guardar secreto sobre la información que el paciente le haya confiado o que hayan podido deducir o interpretar[1991]. Esta obligación se extiende a todo aquél que colabore con el médico[1992]. El incumplimiento por el personal estatutario de este deber de secreto es considerado por el ordenamiento como una falta muy grave[1993].

El deber de secreto se regula, por lo tanto, en la normativa de protección de datos y en la normativa sanitaria. Sin embargo, la perspectiva desde la que se observa en cada una de ellas es diferente. En el segundo caso la obligación surge como consecuencia de las características de un trabajo concreto, que hace que el profesional tenga acceso a determinada información. La relevancia del secreto en el ámbito de la sanidad se ha puesto de manifiesto en numerosos trabajos[1994]. Se trata de un instrumento de gran importancia práctica en la medida que refuerza la relación de confianza que se ha de generar entre profesional sanitario y paciente. En este sentido, el secreto médico cuenta con una relevancia y connotación particular, debido a la función que cumple en el sector en el que surge[1995]. Por el contrario, en las normas de protección de datos la obligación se impone, en términos generales, sobre la información a la que se tiene

[1985] Artículo 197.3 CP.

[1986] Artículo 7.3 LO 1/1982, 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

[1987] Artículo 7.1 RD 33/1986, 10 de enero, por el que se aprueba el Reglamento de Régimen Disciplinario de los Funcionarios de la Administración del Estado: "*Son faltas graves: j) No guardar el debido sigilo respecto a los asuntos que se conozcan por razón del cargo, cuando causen perjuicio a las Administraciones o se utilice en provecho propio*".

[1988] Artículo 7 LBAP: "*1. Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley; 2. Los centros sanitarios adoptarán las medidas oportunas para garantizar los derechos a que se refiere el apartado anterior, y elaborarán, cuando proceda, las normas y los procedimientos protocolizados que garanticen el acceso legal a los datos de los pacientes*". Artículo 19 LBAP: "*El paciente tiene derecho a que los centros sanitarios establezcan un mecanismo de custodia activa y diligente de las historias clínicas. Dicha custodia permitirá la recogida, la integración, la recuperación y la comunicación de la información sometida al principio de confidencialidad con arreglo a lo establecido por el artículo 16 de la presente Ley*".

[1989] Artículo 2.7 LBAP: "*La persona que elabore o tenga acceso a la información y la documentación clínica está obligada a guardar la reserva debida*"

[1990] Artículo 10.3 LGS: "*A la confidencialidad de toda la información relacionada con su proceso y con su estancia en instituciones sanitarias públicas y privadas que colaboren con el sistema público*".

[1991] Artículo 14 Código de Ética y Deontología Médica, 1999.

[1992] Artículo 15 Código de Ética y Deontología Médica, 1999.

[1993] Artículo 72.2.c) 55/2003, 16 de diciembre, del Estatuto Marco del Personal Estatutario de los Servicios de Salud.

[1994] CRIADO DEL RÍO, *Aspectos médico-legales…,* cit., 1999, p. 149; SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000; DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002; VERDÚ PASCUAL, *Secreto profesional…,* cit., 2005; MÉJICA y RAMÓN DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 105; REQUEJO NAVEROS, *El Delito de Revelación…*, cit., 2006, p. 57.

[1995] OTERO GONZÁLEZ, *Justicia y Secreto…,* cit., 2001, p. 4, se refiere a las particularidades del secreto profesional, que deriva de la relación de confianza que se crea entre diferentes sujetos.

acceso en cumplimiento de unas funciones como responsable o encargado de un fichero o tratamiento, o persona que trabaja para alguno de éstos. En este caso, el deber de secreto no nace de una relación especial, sino del mero hecho de manipular datos de carácter personal[1996]. Resulta evidente la estrecha relación entre los dos tipos de secreto, pues en ambos casos se trata de crear herramientas dirigidas a proteger la intimidad o el derecho a la autodeterminación informativa[1997]. Sin embargo, lo que aquí interesa es analizar no tanto las particularidades del secreto médico, sino la figura del deber de secreto prevista en la normativa de protección de datos, que evidentemente incide en el ámbito sanitario.

De inicio, la interpretación de la regulación que dispone la normativa de protección de datos respecto del deber de secreto no presenta mayores complicaciones. El respeto al derecho a la autodeterminación informativa exige que cuando un responsable de fichero está manipulando determinada información de carácter personal los datos no puedan salir del ámbito de relación entre el titular de los datos, dicho responsable y las personas que están a su servicio[1998]. La obligación que se impone en las normas tiene gran alcance. En primer lugar, porque afecta al responsable o encargado y a toda persona que trabaje para ellos[1999]. Y en segundo lugar, porque la obligación perdura más allá de la relación entre el titular y el responsable, o entre éste último y las personas que trabajan para él[2000].

La importancia de esta figura resulta indiscutible. Como se ha puesto de manifiesto por la jurisprudencia, en las sociedades actuales las nuevas tecnologías acercan la información al ciudadano y cada vez resulta más sencillo acceder a los datos de carácter personal y manipularlos. Ante esta circunstancia el deber de sigilo constituye una garantía jurídica dirigida a que dicha información no salga de determinado ámbito, asegurando la capacidad de control de quien es su titular[2001].

Los problemas de interpretación en relación a este deber de secreto derivan de su relación con la figura de la cesión. De lo dicho hasta ahora parece sencillo concretar la vinculación entre ambos principios. Se acaban de explicar el sentido y la relevancia del deber de secreto[2002]. La

[1996] SAN 18 de julio de 2007, FJ 3: "El deber de secreto en el tratamiento de datos personales, tiene la misma fundamentación jurídica (que el secreto profesional), pero se refiere al ámbito estricto del tratamiento de los datos personales, para que el responsable del fichero y, cualquier persona que intervenga en el tratamiento, esté obligado al mantener la confidencialidad de los datos personales".

[1997] SANZ CALVO, Lurdes, "Deber de Secreto…", cit., 2008, p. 271.

[1998] Resolución AEPD R/00871/2010, procedimiento AP/00094/2009, 7 de mayo de 2010: "Dado el contenido del precepto, ha de entenderse que el mismo tiene como finalidad evitar que por parte de quienes están en contacto con los datos personales almacenados en ficheros se realicen filtraciones de los datos no consentidas por los titulares de los mismos".

[1999] NAVALPOTRO NAVALPOTRO, "El Deber de Secreto…", cit., 2007, p. 571; SAN 9 de julio de 2007: En este caso, el BBVA da información sobre los movimientos de la cuenta de una persona que ha fallecido, a una tercera. FJ 2: "La obligación de secreto profesional en el tratamiento de los datos personales afecta, según se recoge de forma expresa en el precepto, no solo al responsable del fichero, sino a todos los que intervengan en cualquiera de las fases del tratamiento. Es decir, todos los que intervienen en el tratamiento de datos de carácter personal, incluidos en un determinado fichero o que suponga un tratamiento deben guardar secreto, respetando en todo momento su confidencialidad".

[2000] SAN 14 de marzo de 2003, FJ 2.

[2001] SAN 14 de marzo de 2003, FJ 2.

[2002] Resolución AEPD R/00871/2010, procedimiento AP/00094/2009, 7 de mayo de 2010: "El deber de secreto profesional que incumbe a los responsables de los ficheros, recogido en el artículo 10 de la LOPD, comporta que el

obligación de sigilo exige que los datos no salgan de determinado ámbito. Su incumplimiento, por lo tanto, no será otra cosa que sacar a la luz los datos que están siendo tratados dentro de la relación entre un titular de datos y un responsable de fichero. Pues bien, esta acción de sacar a la luz no es más que una transmisión o comunicación, si se entiende ésta en el sentido amplio arriba descrito. Tanto en la comunicación como en el incumplimiento del deber de secreto se estaría difundiendo información de carácter personal, más allá de la esfera inicialmente definida entre un titular de datos y un responsable de fichero. Desde el punto de vista sustantivo resulta evidente que se trata de acciones que están íntimamente relacionadas[2003].

Esta relación, sin embargo, no acaba en el hecho de que se refieran a realidades semejantes. También deriva de la circunstancia de que ambas se someten a un mismo régimen jurídico. Como se ha visto, la regulación del deber de secreto en las normas sobre protección de datos es especialmente escueta. Simplemente se señalan su sentido y alcance, pero nada se dice, por ejemplo, de las circunstancias que pueden justificar la vulneración de dicha obligación. Esto se debe a que el régimen jurídico a aplicar a esta figura es el mismo que concierne a las cesiones. Es lógico que así sea en la medida en que el efecto o resultado de ambas acciones viene a ser el mismo, a saber: que los datos salgan de la relación entre el responsable del fichero y el titular de los datos. Más adelante se analizarán las causas que justifican una cesión de datos: el consentimiento, una norma con rango legal, la persecución de determinados fines, etc. Pues bien, estas mismas causas justifican también el que se pueda romper el deber de secreto. Esta circunstancia se ha puesto de manifiesto tanto en la jurisprudencia como en diferentes resoluciones de la AEPD[2004]. En el ámbito sanitario, las causas que motivan que unos datos puedan ser comunicados a un tercero justificarán también la ruptura del deber de secreto[2005].

Ambas figuras aparecen estrechamente relacionadas. Más allá de esta evidente vinculación, los problemas surgen en el momento en que la cesión y el incumplimiento del deber de secreto pueden ser confundidos. La normativa de protección de datos permite una interpretación especialmente amplia del concepto de cesión, que llega a abarcar todo supuesto en que los datos de carácter personal salen a la luz, independientemente de que exista o no un cesionario que recoja dicha información para su posterior tratamiento. La cesión abrazaría incluso los casos en que los datos simplemente se publican o se difunden por cualquier medio, sin un destinatario concreto. Pues bien, estos supuestos son los que en principio protege el deber de secreto. Si se

responsable o quienes intervengan en cualquier fase del tratamiento de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el "deber de guardarlos, obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo".

[2003] MARÍN PÉREZ, "El deber de secreto…", cit., 2010, p. 941; TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 950.

[2004] SAP de Asturias 19 de abril de 2005, FJ 4; SAP de Madrid 19 de octubre de 2004, se refiere al caso en que un investigador cuelga en Internet la HC de un paciente. FJ 2: se refiere la Audiencia, en este caso, a que la difusión de datos de salud por Internet puede vulnerar el artículo 10 LOPD, en la medida en que dicha difusión no encuentra justificación en ninguno de los supuestos recogidos en el artículo 11. Resolución AEPD R/00791/2010, procedimiento AP/00067/2009, 6 de abril de 2010: "El Art. 10 de la LOPD regula de forma concreta el deber de secreto de quienes tratan datos personales, dentro del título dedicado a los principios de protección de datos. Este deber de secreto pretende que los datos personales no puedan conocerse por terceros, salvo de acuerdo con lo dispuesto en otros preceptos de la LOPD, como el Art. 11 *(comunicación de datos)* ó 12 (acceso a los datos por cuenta de terceros)"; Resolución AEPD R/01133/2009, procedimiento AP/00062/2008, 22 de abril de 2009.

[2005] Resolución AEPD R/00192/2010, procedimiento AP/00080/2009, 1 de marzo de 2010.

asumiera la interpretación amplia del concepto de cesión sería fácil confundir el incumplimiento del deber de secreto y la cesión. Así ha sucedido en algunos informes jurídicos de la AEPD, en los que se ha interpretado que supuestos en que la mera difusión de unos datos, sin determinar un cesionario concreto que vaya a manipular la información transmitida, constituyen cesión de datos[2006]. El problema surge por el hecho de que con la interpretación amplia de la cesión la figura del deber de secreto y las sanciones al incumplimiento de esta obligación dejarían de tener sentido en la LOPD, pues el ámbito que protegen resultaría ya protegido por la regulación que la normativa hace de la cesión.

Ante esta situación es necesario dar un contenido propio al deber de secreto y realizar una interpretación adecuada del concepto de cesión, con el fin de que los preceptos que en la LOPD regulan el deber de secreto no carezcan de sentido propio. La distinción entre dichas figuras ha sido señalada desde diferentes fuentes. La jurisprudencia ha concluido que para que se pueda hablar de cesión es necesario reconocer en la transmisión de datos un "elemento volitivo cualificado": que el cedente haya previsto que el cesionario empleará los datos con un fin concreto. Mientras tanto en el caso de la vulneración del deber de secreto no existiría esa voluntad[2007]. Diferentes resoluciones de la AEPD han hecho suya esta interpretación[2008]. También la doctrina ha seguido en algunos casos este criterio. Se ha señalado que en el caso de la cesión debe aparecer el elemento volitivo de transmitir la información para que un tercero la manipule, mientras que en la revelación no se reconoce dicho elemento[2009]. La cesión requeriría de cedente y cesionario, mientras que en el incumplimiento del deber de secreto no se daría esta circunstancia concreta[2010].

Siguiendo esta línea de interpretación se admitiría el concepto restrictivo de cesión, limitando su aplicación a los casos en que se da una relación entre un cedente y un cesionario que recabará los datos nuevamente para llevar a cabo un nuevo tratamiento. El deber de secreto se referiría a los supuestos en que la información de carácter personal sale, simplemente, a la luz, sin que se dirija a un destinatario determinado para que la manipule. En la mayoría de casos, el incumplimiento de secreto se dará cuando los datos son difundidos o publicados en tablones de

[2006] Informe jurídico AEPD, "Difusión de datos de sentencias condenatorias por negligencia médica", 2000; Informe jurídico AEPD, "Publicación de datos en procesos selectivos", 2007; Informe jurídico AEPD, 0074/2009

[2007] SAN 9 de noviembre de 2005, FJ 4.

[2008] Resolución AEPD R/00604/2010, procedimiento AP/00063/2009, 16 de marzo de 2010: "Debe compararse el texto de los artículos 10 y 11 de la LOPD, que definen, respectivamente, los deberes de secreto profesional respecto de los datos de carácter personal que integran el fichero y la prohibición de comunicación, salvo los supuestos previstos, de dichos datos, pues la trasgresión de cualquiera de dichas garantías por parte de quien se responsabiliza del fichero supone, desde un punto de vista meramente fáctico, una conducta semejante: la comunicación de la información que se contiene en el fichero. Así, la distinción entre ambos tipos de garantías exige que la cesión suponga un comportamiento cualificado de la comunicación de datos, cualificación que no puede ser otra que la voluntad de que los datos sirvan para ser tratados de forma automatizada por parte del cesionario, en este caso la UPV, circunstancia que no concurre en este caso, por lo que la comunicación acontecida debe encuadrarse dentro del marco del deber de secreto recogido en el artículo 10 de la LOPD"; Resolución AEPD R/00625/2010, procedimiento AP/00083/2009, 12 de marzo de 2010.

[2009] GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, pp. 288-289, que hace suyas las palabras de APARICIO SALOM al respecto.

[2010] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 66-67.

anuncios, en medios de comunicación, o son depositados en lugares públicos[2011]. Con la configuración de dos espacios diferentes en el que pueden actuar la cesión y el deber de secreto se acaba otorgando sentido al articulado de la LOPD, dando personalidad propia a los preceptos 10 y 11.

Parte de la doctrina ha empleado recientemente un criterio distinto al que se acaba de exponer para distinguir las dos figuras. Se ha apuntado que la diferencia deriva del hecho de que en la cesión de datos la revelación se produce debido a un tratamiento de datos, mientras que en el incumplimiento del deber de secreto dicha revelación se produciría sin que mediara un tratamiento[2012]. La existencia de una cesión no dependería, como se ha hecho ver hasta ahora, de la existencia de un cesionario concreto. Lo que identificaría la cesión sería que la transmisión se produjera a través de una acción que pudiera identificarse como un tratamiento, independientemente de que el cesionario fuera identificado o no. Siguiendo este criterio cabría entender que hay cesión en una publicación a través de Internet. Se cree aquí que esta interpretación plantea problemas prácticos, de aplicación. Este criterio plantea la dificultad de distinguir, a efectos de aplicar la LOPD, supuestos en que se está ante un tratamiento y situaciones en las que no. Teniendo en cuenta la especialmente amplia definición que se ha dado del concepto de tratamiento no resultaría fácil identificar, aplicando el último criterio expuesto, los casos en que se está ante un simple incumplimiento del deber de secreto en vez de ante una cesión. Es por ello que se entiende aquí conveniente abogar por la aplicación del criterio planteado más arriba para distinguir la cesión y el incumplimiento del deber de secreto, basado en la existencia o no de una voluntad del cedente de transmitir los datos a un cesionario.

Sea como sea, lo realmente relevante de la regulación que recoge la normativa de protección de datos es, que mediante la cesión y el deber de secreto se otorga un importante sistema de garantías al titular de los datos cada vez que éstos se transmiten. Más allá de la confusión que la letra de la LOPD puede generar a la hora de aclarar dichos conceptos, la Ley da cobertura a todas las operaciones en que los datos salen de la inicial esfera en que se están tratando. Tanto cuando la información se dirige a un destinatario determinado, como cuando el cesionario es, o puede ser, indefinido o desconocido, toda transmisión ha de cumplir una serie de requisitos que aseguran que la operación se lleve a cabo con las garantías oportunas[2013]. Estos requisitos serán los mismos para la cesión y el incumplimiento del deber de secreto, a pesar de constituir figuras diferentes. Es por ello que se analizarán en este apartado dedicado a la cesión, sin que sea necesario dedicar un epígrafe específico al deber de secreto.

[2011] STS 2 de junio 2010, FJ 1, se sanciona el depositar historias clínicas en la basura. SAN 1 diciembre de 2009, FJ 4, en la que se sanciona el que profesionales de la sanidad difundan datos sanitarios de determinados pacientes en los tablones de los centros. SAN 2 de julio de 2009, FJ 3, en la que se sanciona el colgar en Internet datos sanitarios relativos a consultas de interrupción voluntaria de embarazo. Resolución AEPD R/00801/2010, procedimiento PS/00677/2009, 7 de mayo de 2010, caso en que se publican datos en el tablón de un portal al que tienen acceso los vecinos; Resolución AEPD R/00795/2010, procedimiento PS/00553/2009, 6 de abril de 2010, caso en que una entidad bancaria remite a sus empleados por correo electrónico datos de otros empleados. Resolución APDCM 14 de junio de 2010, "Fichero compartido en la red Emule con registro de datos personales y médicos".
[2012] TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 951.
[2013] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 38.

I.3.1.D. Breve referencia a la distinción entre la cesión y el acceso a los datos por cuenta de terceros.

Para completar la definición de la cesión es necesario hacer un primer acercamiento al concepto de acceso a los datos por cuenta de terceros[2014], sin perjuicio de que más adelante se lleve a cabo un análisis más exhaustivo sobre esta figura.

Es común que, sobre todo por dificultades técnicas y falta de conocimiento, tanto empresas privadas como administraciones públicas externalicen el servicio de tratamiento de la información de que disponen[2015]. La obligación de cumplir con la LOPD, sobre todo con las medidas de seguridad que impone la Ley, hace que se acuda a empresas especializadas en otorgar ese tipo de servicios. Puede suceder que lo externalizado sea otro servicio distinto que requiere a su vez del tratamiento de datos. En el sector sanitario esta operación no resulta extraña. Para que estas empresas externas puedan desarrollar su trabajo es necesario, como es lógico, que tengan acceso a la información de que dispone el responsable del fichero que contrata dicho servicio. ¿Se considera este acceso una cesión de datos?

Cuando se habla de la cesión se hace referencia generalmente a que un tercero se hace con los datos de carácter personal, de forma que pueden ser manipulados por éste, como nuevo responsable, con una nueva finalidad que nada tiene que ver con la que inspiraba el primer tratamiento. El nuevo responsable, el cesionario, decide sobre los datos que se le han transmitido y lleva a cabo una nueva manipulación. Por el contrario, en el acceso por cuenta de tercero el destinatario no se convierte en responsable, pues no fija la finalidad del tratamiento, sino que está sometido a lo que el responsable del fichero decida sobre el mismo. El responsable es el que determina cómo hay que tratar los datos, mientras que el tercero, que adquiere el calificativo de encargado de tratamiento[2016], es el que materialmente realiza dicho tratamiento de acuerdo a lo que dicta el responsable[2017]. El encargado no lleva a cabo una nueva manipulación, distinta a la realizada por el responsable, sino que emplea los datos en nombre de aquél. Se trata de la "colaboración de un tercero que le preste el servicio (al responsable del fichero) – por no disponer de las necesarias aplicaciones informáticas o por meras razones de conveniencia- de tratamiento automatizado de estos datos de carácter personal"[2018].

El elemento principal que determina la existencia de la externalización u *outsourcing* es la formalización de un contrato entre el responsable del fichero y el encargado del mismo, que será quien lleve a cabo el tratamiento de los datos[2019]. En este contrato se establecerán las cláusulas que marcarán cómo ha de llevarse a cabo dicho tratamiento por parte del encargado. En la

[2014] Artículo 12 LOPD.
[2015] DEL PESO NAVARRO, *Manual de Outsourcing…,* cit., 2003, p. 5; AIBAR y URGELL, *Estado, Burocracia…,* cit., 2007, pp. 48 y 49.
[2016] Artículo 3.g) LOPD: "*Encargado de tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento*".
[2017] SAN 21 de junio de 2002 FJ 6.
[2018] SAN 12 de abril del 2000, FJ 3.
[2019] WHITE y JAMES, *Manual del Outsourcing…,* cit., 2000, p. 15; MESSÍA DE LA CERDA, *La cesión o comunicación…,* cit., 2003, p. 166.

medida en que este último actúe dentro de los criterios marcados en el contrato será el responsable del fichero el que responderá por la actuación del encargado. En caso de que el encargado actúe fuera de los criterios señalados por el contrato será éste el que deberá responder por su actuación y no el responsable. Si no hay contrato no hay *outsourcing*. Si el responsable del fichero transmite los datos a un pretendido encargado, pero lo hace sin fijar en un contrato las cláusulas que han de guiar el tratamiento de datos por parte de este último, dicha transmisión será una cesión común. En este caso será necesario que se cumplan todos los requisitos que una cesión exige, fundamentalmente el consentimiento del titular[2020].

I.3.2. Una aclaración sobre el concepto de cesión en el ámbito sanitario.

La definición que se ha dado del concepto de cesión, y también la dada del deber de secreto, tienen perfecto encaje en el ámbito sanitario. La importancia de sujetar a determinadas reglas todo tipo de transmisión de los datos se acentúa en este campo. Hay que recordar los efectos negativos que puede tener un uso incorrecto por parte de terceros de los datos de salud, incluso, como se ha puesto de manifiesto en alguna ocasión, a la hora de ejercer otros derechos fundamentales[2021]. Las transmisiones, cualquiera que sea la fórmula empleada para llevarlas a cabo, multiplican el riesgo de que se produzcan esos efectos.

En el ámbito sanitario, sin embargo, el concepto de cesión plantea un problema de relevancia. Se trata de la dificultad de concretar si determinadas operaciones constituyen cesión o no. En la práctica sanitaria los datos que aportan los usuarios se trasladan a ficheros a los que diferentes sujetos, incluso profesionales que no se dedican a la asistencia sanitaria directa, pueden llegar a tener acceso: otros médicos, personal administrativo, de enfermería, investigador, etc. Estos sujetos accederán a la información para cumplir las funciones que les corresponden. Son múltiples las operaciones que se realizan sobre la información sanitaria contenida en los diferentes ficheros de los que son titulares los sistemas sanitarios. En la medida en que un tercero, distinto al médico al que generalmente el paciente transmite inicialmente los datos, se hace con los datos estos accesos podrían ser considerados como cesiones de datos. Sin embargo, cabe preguntarse si esto es realmente así. ¿Es el acceso por parte de los profesionales de la sanidad a una historia clínica una cesión de datos? ¿Constituye el acceso por parte de personal investigador a esta misma información una cesión de datos? ¿Es una cesión el acceso por parte del personal administrativo a los datos que estime necesarios para desarrollar su labor de gestión? Se entiende aquí que muchas veces estas operaciones no constituyen una comunicación sino un mero acceso por profesionales que tienen que cumplir su función. Estas acciones podrán ser consideradas o no cesiones de datos dependiendo de las circunstancias[2022].

Desde un punto de vista estrictamente jurídico la importancia de determinar cuándo se está ante una cesión es de gran alcance, pues en ese caso será de aplicación la regulación correspondiente a esta figura en la Ley. Ello supondrá ante todo tener que cumplir con el

[2020] SAN 6 octubre 2004, FJ 4.
[2021] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 14.
[2022] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, p. 41.

requisito de solicitar el consentimiento del titular de los datos para llevar a cabo la cesión o tratar de encajar esta operación en alguno de los supuestos que excepcionan dicha exigencia.

Desde un punto de vista práctico, el que se entienda que los accesos que se han planteado constituyen cesiones de datos podría llevar a ralentizar y, quizás, entorpecer la práctica sanitaria. Tratar de encontrar el consentimiento del titular de los datos para poder llevar a cabo cada uno de dichos accesos, o intentar encajar cada una de esas operaciones en alguno de los supuestos que excepciona el requerimiento del consentimiento, dificultaría el trabajo de los profesionales sanitarios. Por el contrario, si se entiende que esas acciones constituyen un mero acceso se facilitará y agilizará la labor de los profesionales, que se despreocuparán de la necesidad de conocer si están respetando el derecho de los usuarios a consentir o no. Este hecho hay que tenerlo en cuenta a la hora de interpretar lo que es cesión en este ámbito.

El ordenamiento no aclara demasiado cuál ha de ser el criterio que lleve a determinar cuándo se está ante una comunicación en el ámbito sanitario y cuándo no. Tampoco la doctrina ha entrado con profundidad a resolver esta cuestión. Se entiende aquí que a la hora de concretar lo que es cesión en la práctica sanitaria hay que atender a las normas que crean estos ficheros. En éstas se fijará cuál es el ámbito de utilización de los datos sanitarios. La determinación, sobre todo, de quién es el responsable del fichero y de la finalidad a la que se destinará la información dará la clave para concluir cuándo se está ante una cesión y cuándo no[2023].

En alguna ocasión se ha interpretado que el que una acción sea considerada como acceso o comunicación pudiera depender del hecho de que el sistema de información sanitario sea centralizado o descentralizado[2024]. Si se ha entendido bien este planteamiento parte de la idea de que en los sistemas centralizados se crea una base de datos única, en la que se cuenta con información sanitaria que puede ser empleada para llevar a cabo diferentes fines, a la que tienen acceso distintos agentes. Los pacientes tendrían conocimiento de estas finalidades. Los profesionales, por su parte, tendrían sus funciones bien definidas y accederían a determinados datos para llevar a cabo dichas tareas. El acceso se limitaría a una serie de datos. Estas operaciones no constituirían cesiones, pues se trataría de manipulaciones realizadas directamente sobre la base de datos por profesionales en el cumplimiento de sus funciones. Realmente no habría transmisiones, sino meros accesos a esa base de datos única.

[2023] APDCM, *Protección de datos…,* cit., 2008, p. 223: "¿Quién es el responsable de los ficheros que se utilizan en un centro o institución pública prestadora de servicios sanitarios?
En los ficheros de titularidad pública, el responsable del fichero es el órgano administrativo que trata la información y tiene competencias en la materia, teniendo capacidad de decidir sobre el contenido, finalidad y uso del tratamiento de datos que se realiza".

[2024] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, pp. 43-44; TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 83: "El acceso a la historia clínica será un supuesto de acceso o de cesión dependiendo de que la historia clínica se encuentre descentralizada por centros o por áreas o se encuentre centralizada. En el primer supuesto se tratará de una cesión de datos sin consentimiento del interesado habilitada por Ley; en el segundo supuesto se trataría de un acceso legítimo al fichero centralizado de historias clínicas dentro del marco del principio de calidad". Si bien en otros casos no se ha apostado por seguir esta línea interpretativa: TRONCOSO REIGADA, "El principio de calidad…", cit., 2010, p. 385, donde parece señalarse que la cesión se da cuando hay una transmisión de datos entre entidades que tienen personalidad jurídica propia. En el caso de las administraciones habrá cesión cuando la transmisión se produzca entre administraciones diferentes; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 442-444.

Se cree que esta interpretación pasa por alto la práctica diaria en los sistemas de información centralizados, en los que las transmisiones entre centros, entre éstos y ambulatorios, entre profesionales sanitarios, y entre éstos y personal administrativo generan situaciones que han de estar necesariamente sujetas a un régimen más riguroso que el que sugiere o conlleva un mero acceso. Cabría preguntarse si en un sistema centralizado el acceso de personal de la división o área de gestión económica a datos sanitarios contenidos en la base de datos única, pero de los que es responsable la división de asistencia sanitaria, se consideraría un mero acceso. Se entiende aquí que no. A pesar de tratarse de un sistema centralizado, el acceso de este agente para manipular datos sanitarios de los que no es responsable, con una finalidad no sanitaria, constituye una cesión. En el sistema centralizado pueden encontrarse diferentes carpetas con datos de diferentes características que pueden ser empleados con distintos fines. De inicio, cada agente tiene definidas sus funciones y los accesos que le son permitidos. Si un agente tiene acceso a una carpeta que se sitúa fuera de su campo de acción, en principio se tratará de una cesión de datos, independientemente de que sea necesario el consentimiento del titular de los datos o no. Así, el acceso de personal administrativo a datos sanitarios de un paciente contenidos en un fichero que se sitúa fuera de su ámbito de actuación, sea en un sistema centralizado o descentralizado, no puede sino considerarse como una cesión de datos. Lo contrario podría suponer que datos que se recogen para ser incluidos en la base de datos centralizada con fines estrictamente sanitarios pudieran ser objeto de accesos, no considerados cesiones, dirigidos a cumplir los más diversos fines, sin necesidad de recabar el previo consentimiento del titular de los datos ni justificar debidamente el tratamiento. No parece que de partida este planteamiento otorgue las suficientes garantías al derecho a la autodeterminación informativa de los pacientes y usuarios de un sistema sanitario determinado.

En otros casos se ha entendido que el que haya cesión dependerá de si la transmisión se realiza entre entidades con personalidad jurídica propia o no. Las transferencias de datos entre órganos o unidades de una misma Administración, por ejemplo, no serían cesión sino meros accesos[2025].

Se entiende aquí que la interpretación del concepto jurídico de cesión ha de responder a argumentos más complejos. Los accesos no serán cesiones siempre y cuando se den en cumplimiento de las finalidades que marca la norma de creación del fichero correspondiente, finalidades que justificaron la recogida de los datos y sobre las que se ha informado al usuario, y se produzcan dentro del campo de acción del responsable del fichero designado en la propia norma de creación. Fuera de los usos previstos en la norma de creación y de la esfera de actuación de ese responsable del fichero toda transmisión o acceso será considerado cesión de datos, siéndole de aplicación la normativa correspondiente a esta operación. Sería el caso, por ejemplo, en que un Juez o Tribunal solicita acceder a la historia clínica para que un procedimiento pueda desarrollarse con todas las garantías, o los casos en que datos de este fichero se han de trasladar a otro centro, de otra comunidad autónoma por ejemplo, para asistir al titular de los datos fuera de esta comunidad, o los supuestos en que dentro de un mismo sistema

[2025] TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 442-444.

sanitario se emplean datos recogidos en un fichero por un tercero que no es el responsable, para llevar a cabo finalidades que no corresponden a dicho responsable.

Se puede trasladar lo dicho a los ficheros de datos creados en el sistema sanitario del País Vasco. Si se atiende a la norma que crea estas bases de datos se observa que sólo se consideran cesiones las transmisiones a organismos situados fuera de esta Administración. Es el caso del ya citado Registro de Casos de Sida en la que la única cesión que se prevé es la que se pueda realizar al Ministerio de Sanidad y Consumo[2026]. Fuera de estos supuestos las transmisiones no serían, según la propia norma, cesiones, sino meros accesos. De esta forma, los flujos de datos que se puedan dar entre las distintas divisiones que componen la propia Administración no constituirían cesión de datos. El acceso de personal administrativo del mismo centro a datos sanitarios contenidos en las historias clínicas no constituiría una comunicación. Sin embargo, más allá de posibles cesiones a otras administraciones, estos ficheros reconocen múltiples finalidades a las que se podrán destinar los datos sanitarios que contienen: investigación, estadística, etc. Estas finalidades en ocasiones se llevarán a cabo por órganos que pertenecen al departamento responsable del fichero y a veces por otros órganos que no están considerados en la norma como tales, pero que pertenecen a la misma Administración. Estos accesos no son considerados en la norma creadora de los ficheros como cesiones. Partiendo de lo que se ha dicho aquí sobre lo que ha de entenderse como cesión, la regulación realizada por la norma vasca no es correcta.

El hecho de que en la norma que crea los ficheros no se califiquen unas acciones determinadas como cesiones no significa que no lo sean. Si unos datos que son recogidos por un responsable son remitidos a otro para que los emplee con una finalidad distinta a la perseguida por el primero, esta acción no podrá considerarse de otra manera que no sea una cesión, por mucho que no haya sido calificada así en la norma creadora del fichero. Hay que tener en cuenta que cada finalidad cuenta con una regulación determinada: no es lo mismo que los datos se empleen para llevar a cabo la asistencia sanitaria directa o para realizar actividades de docencia. En el primer caso la excepción al consentimiento podría justificarse con facilidad, mientras que en el segundo resultaría más complicado. Si unos datos son empleados por un responsable para llevar a cabo una finalidad y más adelante se utilizan por otro para cumplir otro objetivo, necesariamente habrá habido una cesión de datos.

Si se atiende, por ejemplo, al fichero denominado Historial Clínico de Osakidetza, se verá que la responsable del fichero es la División de Asistencia Sanitaria de esta institución. En principio, por lo tanto, parece que todo uso que se pueda dar dentro de esa división para cumplir sus finalidades, sea dirigida a la asistencia primaria o especializada, no constituye cesión de datos sino acceso por parte de los profesionales sanitarios para desarrollar su trabajo de salvaguarda de la salud de las personas. Esto no quiere decir, como se verá, que cualquier profesional sanitario pueda tener acceso a la historia clínica completa de cada paciente. Cada uno, de

[2026] El fichero denominado Registro de Casos de Sida, por ejemplo, recoge expresamente cesiones al Ministerio de Sanidad y Consumo. Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de salud.

acuerdo con sus funciones, deberá tener un acceso determinado. La norma de creación de este fichero no prevé cesiones de los datos contenidos en el mismo. Sin embargo, si se atiende a las finalidades que justifican la recogida de estos datos sanitarios se verá que el tratamiento de esta información va más allá del uso estrictamente asistencial, dirigiéndose también a fines de docencia, gestión financiera o estadística[2027]. Cabe preguntarse si el que la información contenida en este fichero se emplee con fines docentes o de gestión financiera no constituye una cesión de datos. Siguiendo lo defendido en este trabajo hasta ahora, se entiende que si los datos salen de la esfera de la citada División de Asistencia Sanitaria para que sean manipulados por otro órgano, como puede ser la División de Gestión, se está llevando a cabo una cesión de los datos. La información contenida en la historia clínica sale del ámbito de actuación del responsable del fichero, que es la División de Asistencia Sanitaria[2028]. Incluso tratándose de transmisiones realizadas para ejecutar finalidades previstas en la propia norma de creación del fichero, se entenderá que hay cesión en la medida en que los datos salen del ámbito de actuación del responsable[2029]. Así, será de aplicación el régimen jurídico dirigido a regular esta figura, de manera que para que esta comunicación se pueda producir sin el necesario consentimiento del titular de los datos deberá darse alguno de los supuestos que justifican la excepción a ese derecho.

I.4. El contenido de la cesión.

Una vez determinado el concepto, corresponde analizar los requisitos que las normas exigen para que una cesión de datos sea válida. La LOPD requiere fundamentalmente que medie el consentimiento previo del interesado y que los fines que justifican la cesión estén directamente relacionados con las funciones legítimas del cedente y del cesionario[2030]. La ley exige también que se informe al titular de los datos sobre la finalidad a la que se destinarán los datos que se pretenden comunicar o el tipo de actividad que desarrolla aquél a quien se transmiten[2031]. En definitiva, se trata de tres requisitos fundamentales: consentimiento, información y respeto al principio de finalidad.

I.4.1. El consentimiento.

La cesión exige un consentimiento distinto al que justificó la primera manipulación de los datos. Ha señalado la jurisprudencia que “la cesión (...) supone una nueva posesión y uso que requiere el consentimiento del interesado”[2032]. En la medida en que la comunicación de unos datos lleva a que vayan a ser objeto de un nuevo tratamiento, esta operación requerirá de la aprobación del titular. No basta por lo tanto con el consentimiento recabado en un inicio para el

[2027] Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de salud, por el que se regulan los ficheros de carácter personal gestionados por Osakidetza-Servicio Vasco de salud.
[2028] Acuerdo de 25 de noviembre de 1997, del Consejo de Administración del Ente Público Osakidetza-Servicio vasco de salud, por el que se aprueba la Estructura Orgánica de la Organización Central del Ente Público, en el que se distinguen los órganos a los que se alude, BOPV nº 229, 28 de noviembre de 1997.
[2029] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 83.
[2030] Artículo 11.1 LOPD. SAN 31 de octubre del 2000, FJ 2.
[2031] Artículo 11.3 LOPD.
[2032] STSJ de Madrid 15 de enero de 2004, FJ 6.

tratamiento general de unos datos, sino que es necesaria otra autorización dirigida concretamente a permitir la transmisión.

Se puede plantear si en el caso en que una persona autoriza un tratamiento, a sabiendas de que dicha manipulación incluye futuras cesiones de los datos, este consentimiento inicial legitima dicha transmisión. Muchas veces, en las normas de creación de ficheros públicos ya se prevén las cesiones futuras que se pretenden realizar[2033]. En la medida en que el titular de dichos datos está informado de esta circunstancia y autoriza su tratamiento, se podría pensar que ese consentimiento inicial es suficiente para llevar a cabo las comunicaciones previstas. Se interpreta, sin embargo, que de una interpretación literal de la Ley se deduce que toda cesión de datos, independientemente de si el titular ha sido previamente informado o no sobre la misma, requiere su consentimiento concreto e individualizado.

Hay que tener en cuenta que, la mayoría de las veces, cuando una persona autoriza un tratamiento determinado de sus datos en el que se prevé una futura cesión, la información que se le otorga sobre las características de dicha futura cesión es muy limitada. Normalmente, el responsable que recaba los datos, cuando informa al titular sobre las características que va tener el tratamiento que va a llevar a cabo, remite una información muy general sobre las cesiones que pretende realizar en un futuro. Lo más común es que se limite simplemente a citar la existencia de dichas transmisiones futuras y no se informe sobre las características concretas y detalladas que va a tener la futura comunicación, como la finalidad a la que se destinarán los datos una vez los obtenga el cesionario o la identidad de este último. Es por ello que se entiende exigible en todo caso que siempre que se vaya a llevar a cabo una cesión de datos se recabe la autorización previa del titular, más allá de que éste haya sido previamente informado sobre la existencia de las transmisiones. Indudablemente esta exigencia otorga un mayor control al titular sobre sus datos.

El consentimiento que valide la cesión debe cumplir con una serie de requisitos. Tiene que ser, en primer lugar, previo a dicha operación[2034]. Ya se dijo en su momento que todo consentimiento dirigido a legitimar cualquier tratamiento tiene que ser previo. Sin embargo, es reseñable que en el caso de la cesión, al contrario de lo que ocurría en la regulación del consentimiento común en el artículo 6 de la LOPD, se especifique de forma expresa este requisito[2035], pues demuestra la especial importancia que se le otorga en la norma. A través del cumplimiento de esta exigencia se garantiza que el titular de los datos controle desde el primer instante las circunstancias que rodean a toda transmisión de sus datos.

Respecto a la necesidad de que sea previo, se plantea alguna duda cuando se trata de la cesión de los ficheros privados. Para estos casos, la Ley exige que se informe al interesado

[2033] Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud, por el que se regulan los Ficheros Automatizados de Datos de Carácter Personal gestionados por Osakidetza-Servicio Vasco de Salud, en el que se prevé la creación del fichero llamado "Registro Hospitalario de Tumores" donde se recogen datos de las personas diagnosticadas de cáncer en los hospitales de Osakidetza. Para estos datos se prevén cesiones. Sin embargo, a la hora de describir dichas transmisiones de datos sólo se señala que se tratarán de cesiones nacionales.

[2034] SAN 30 de junio de 2004, FFJJ 5 y 6. BUISÁN GARCÍA, "Comunicación de datos...", cit., 2008, p. 291.

[2035] Artículo 11.1 LOPD.

sobre la transmisión "*en el momento en que se efectúe la primera cesión*"[2036]. La referencia a dicho momento puede llevar a entender que la información se podrá dar después de efectuar la primera cesión. Podría darse en el momento, pero a continuación de producirse la comunicación. No parece que esta posibilidad sea admisible. Como se apuntaba al analizar el derecho a ser informado[2037], no es asumible que una operación que requiere el consentimiento del titular pueda iniciarse sin dicha autorización. Si esta situación se diera podrían ocurrir dos cosas: que se lleve a cabo una cesión de datos sin la autorización del titular pero que posteriormente el titular valide dicha operación. En este caso no habría problema alguno, pues el afectado se muestra partidario de la cesión. Y lo contrario, es decir, que se dé la cesión y que posteriormente el titular rechace la misma. Admitir esta posibilidad abre las puertas a que se lleven a cabo tratamientos de datos que el titular no quiere que se hagan efectivos, sin que tenga conocimiento de los mismos. La inseguridad que genera la posibilidad de que se cedan datos sin el previo consentimiento del titular, cuando es requerido, independientemente de que en algunos casos la comunicación pudiera ser validada posteriormente por el propio titular, no es asumible. El derecho a la autodeterminación informativa ha de hacerse efectivo antes de que tenga inicio el tratamiento de los datos. Por lo tanto, deberá prevalecer la regla general impuesta por el artículo 11 que requiere el consentimiento previo del titular[2038].

En segundo lugar, el consentimiento ha de guardar una forma determinada. Con respecto a este punto no se especifica nada en la Ley. No se dice si ha de ser inequívoco, si basta con que sea tácito, o si tiene características distintas al consentimiento genérico regulado en el artículo 6 de la LOPD. Ante este silencio parece claro que serán de aplicación las disposiciones que regulan el consentimiento común. En este sentido, en lo que corresponde a los datos de salud, tal y como recoge la Ley, el consentimiento tendrá que ser expreso. Ya se analizaron las características que ha de guardar esta autorización expresa al estudiar el principio del consentimiento, por lo que se hace una remisión a lo dicho entonces.

En tercer lugar, este consentimiento, al igual que el reconocido para todo tratamiento de datos, es revocable[2039]. En este caso, al contrario de lo que ocurría en la regulación del consentimiento, la Ley no exige expresamente causa de justificación para llevar a cabo esta acción. No obstante, resulta fácilmente deducible que la exigencia aplicable al consentimiento común o general puede trasladarse también a la cesión de datos. Así lo ha reconocido la doctrina[2040]. De este modo, en relación a este punto basta con remitirse a lo dicho al respecto en el análisis que se ha hecho al hablar del consentimiento. Se mostraba entonces el desacuerdo con la necesidad impuesta por la Ley de tener que justificar la revocación, por entender que es contraria a la esencia del derecho que aquí se analiza. Si depende de la mera voluntad del titular de los datos transmitirlos para que sean tratados, la misma voluntad deberá ser la que pueda revocar la autorización, sin necesidad de que trascienda ninguna causa justificativa. Hay que

[2036] Artículo 27.1 LOPD: "*El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario*".
[2037] Artículo 5.4 LOPD.
[2038] APARICIO SALOM, *Estudio sobre la Ley...,* cit., 2000, p. 68.
[2039] Artículo 11.4 LOPD. BUISÁN GARCÍA, "Comunicación de datos...", cit., 2008, p. 309.
[2040] HERRÁN ORTIZ, *El Derecho…,* cit., 2002, p. 236.

recordar que la propia jurisprudencia ha admitido, al analizar la revocación del consentimiento, la necesidad de llevar a cabo una interpretación favorable a los derechos de las personas[2041].

En cuarto lugar, recabar el consentimiento del titular de los datos es obligación del responsable que va a transmitirlos a un tercero, es decir, del cedente. De inicio, y a falta de una causa que justifique lo contrario, dicho responsable no podrá ceder los datos a otra persona sin la aprobación del afectado o interesado. Esto no quiere decir que quien va a recabar los datos a causa de la comunicación, el cesionario, no tiene responsabilidad alguna a este respecto. La LOPD obliga a este último a la observancia de las disposiciones de la Ley[2042]. Entre las obligaciones se encuentra el deber de verificar en todo caso si la cesión se ha llevado a cabo de acuerdo con lo dispuesto en la Ley y, en concreto, si el cedente ha cumplido con la exigencia de recabar el consentimiento informado. Así lo ha exigido expresamente la jurisprudencia[2043]. El cesionario deberá actuar de manera diligente y tratar de verificar si el cedente ha cumplido con lo requerido por la Ley para que la cesión sea válida[2044]. De lo contrario, como han previsto los tribunales, la actuación del cesionario podría interpretarse como una violación al derecho a otorgar el consentimiento[2045]. Hay que tener en cuenta el hecho de que el cesionario se convierte a raíz de la comunicación en nuevo responsable del tratamiento, pudiendo decidir sobre la finalidad del mismo. Esta circunstancia hace que le sea exigible una especial diligencia a la hora de recibir la información. Ello supone, entre otras cosas, tener que verificar si el cedente ha cumplido con la obligación de recabar el consentimiento para la realización de la cesión. Se entiende aquí, al contrario de lo que ha defendido parte de la doctrina[2046], que la inconsciencia, si se debe a causas imputables al propio cesionario, puede ser sancionada.

El incumplimiento del requisito de recabar el consentimiento en la cesión de datos constituye en la LOPD una infracción muy grave, sancionada en consecuencia[2047]. La imposición de esta sanción ha planteado en la práctica algún problema de interpretación vinculado a la aplicación del

[2041] SAN 11 de enero de 2002, FJ 2.

[2042] Artículo 11.5 LOPD: "*Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley*".

[2043] SAN 18 de octubre 2007, FJ 5, en la que se reconoce que "(…) el cesionario lesiona el principio del consentimiento cuando trata y utiliza datos cedidos sin que se haya obtenido el previo consentimiento, con los siguientes argumentos: El art 11.5 de la LOPD establece que el cesionario de los datos de carácter personal se obliga, por el solo hecho de la cesión, a la observancia de las disposiciones de la presente Ley. Por lo tanto, el cesionario, al obtener los datos, queda obligado y comprometido con las garantías de la Ley. Siendo una de ellas el principio de consentimiento o de autodeterminación. (…) Lo anterior es determinante. En efecto, no puede serle exigido al cesionario la obtención del previo consentimiento de los datos cedidos, pues tal obligación es del cedente. Pero si debe serle exigido, conforme a parámetros de razonable diligencia en el mercado de tráfico de datos, que verifique en forma diligente que dicho consentimiento ha sido obtenido. En caso contrario, cuando dolosamente conozca que dicho consentimiento no ha sido obtenido; o no realice una actividad razonable y diligente tendente a verificar la existencia de dicho consentimiento incurriendo en negligencia o culpa, se produce una lesión del principio del consentimiento, pues el cesionario usa de datos, en los que por dolo o culpa no le consta la existencia del previo consentimiento y por lo tanto trata datos en contra de lo manifestado por la persona titular de los datos con lesión de su privacidad."

[2044] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 170; BUISÁN GARCÍA, "Comunicación de datos…", cit., 2008, p. 310.

[2045] SSAN, 15 de septiembre de 2001, FJ 3 y 30 de junio de 2004, FJ 6.

[2046] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 88, apunta que "sólo podrá hacerse una imputación de responsabilidad para el cesionario en el caso que se comenta cuando conozca la falta de autorización para obtener los datos, no en el caso de que sea inconsciente de tal circunstancia".

[2047] Artículo 44.4 LOPD: "*Son infracciones muy graves (...): b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas".*

principio *non bis in idem*. Se ha pretendido en alguna ocasión imponer al sólo y único hecho de ceder unos datos sin el necesario consentimiento del titular una doble sanción. Por un lado, castigando esta acción en base al incumplimiento del artículo 6 de la Ley, en la medida en que se lleva a cabo un tratamiento sin la necesaria autorización del titular de los datos[2048], entendiendo que la cesión no es más que otra forma de tratamiento. Y por otro, sancionando la acción por incumplimiento del artículo 11, que exige también el consentimiento, en este caso, para la cesión propiamente dicha. Un mismo hecho sería castigado dos veces, aplicando distintas disposiciones. Esta circunstancia podría llevar a la aplicación del principio *non bis in idem* para resolver el problema de la imposición de una doble sanción a un sujeto por un mismo hecho[2049]. Ya se comentó al hablar del consentimiento informado las dificultades que plantea la aplicación de este principio. No obstante, en este punto la solución es más sencilla que la prevista para aquél supuesto. Se entiende aquí que más que de una posible aplicación del principio *non bis in idem* se trata de un simple error de concepto. Como ha señalado la jurisprudencia, en caso de no recabarse el consentimiento requerido para llevar a cabo la cesión de datos la sanción se impondrá en razón del incumplimiento del artículo 11 de la Ley, dejando a un lado la que podría derivar del incumplimiento del artículo 6[2050]. Ya se ha apuntado más arriba que el concepto de tratamiento puede tener una acepción amplia y otra más restrictiva. Como se puede suponer, la acción que se sanciona cuando se castiga el tratamiento sin consentimiento no es todo tratamiento, incluyendo la cesión, sino sólo el tratamiento entendido en sentido estricto, que no engloba la cesión. La cesión no es más que una operación más, junto a la recogida y el tratamiento en sentido estricto, que si se realiza de manera contraria a Derecho se sanciona.

I.4.2. El deber de informar sobre la cesión.

La normativa exige que el consentimiento en la cesión de datos sea informado[2051]. Antes de dar su aprobación el titular de los datos deberá conocer los parámetros que rodearán la transmisión. La LOPD, sin embargo, no lleva a cabo una regulación extensa sobre el contenido de la información que se ha de dar al titular. Al referirse a este punto la regulación general de la cesión sólo alude al deber de informar sobre la finalidad. Podría pensarse que en las comunicaciones el interesado sólo deberá ser informado sobre ese elemento. Esta circunstancia podría suponer una injustificada limitación del deber de informar en comparación a lo que se solicitaba para los tratamientos comunes, que ya se ha analizado. Es más, esta previsión chocaría con la que se lleva a cabo sobre la cesión de datos contenidos en ficheros privados, donde el deber de información se extiende a más elementos, exigiéndose que se informe al titular sobre la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario[2052]. La importancia de informar sobre la identidad de quién recaba los datos ha sido puesta de manifiesto por la jurisprudencia, en relación a un supuesto en que una

[2048] Artículo 44.3 LOPD: "*Son infracciones graves (...): c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible*".
[2049] REDONDO ANDREU, "El principio…", cit., 2009, p. 305; CUBERO MARCOS, *El principio…*, cit., 2010, p. 28.
[2050] SAN 3 de septiembre 2007, FJ 2.
[2051] Artículo 11.3 LOPD.
[2052] Artículo 27.1 LOPD.

persona transmitió cierta información sanitaria a una aseguradora, pensando que era aquélla a la que ella se encontraba adscrita, que no informó sobre su identidad[2053].

El contenido del deber de informar al titular de los datos en las cesiones ha de ser más extenso que el que en un inicio pudiera derivarse del artículo 11 de la Ley. La determinación del alcance de este deber de informar ha de tomar en consideración diferentes cuestiones. Primero, como se ha comentado al analizar el derecho a la información, cuando una persona transmite unos datos de los que es titular a un segundo sujeto, este último deberá informar al primero sobre las características del tratamiento que va a dar a esos datos. Entre otras circunstancias, si dicho segundo sujeto pretende ceder los datos recabados a un tercero, deberá informar al titular sobre la transmisión que prevé llevar a cabo. En el momento de la recogida el titular de los datos es informado sobre las cesiones que se van a llevar a cabo de sus datos. ¿Bastaría con esta información para entender cumplida la exigencia normativa? Como antes se dijera, se entiende aquí que no. Hay que tener en cuenta que esta información inicial, que se da cuando el titular transmite los datos al primer responsable de fichero, suele ser especialmente limitada, referida únicamente a la existencia misma de las citadas cesiones, pero sin detallar los distintos aspectos que rodearán la operación. Por lo tanto, esta información inicial no quita para que la regulación de la cesión de datos exija, en el momento en que la transmisión se va a realizar, una información completa sobre dicha comunicación. Esta nueva información, que se da cuando la cesión se va a llevar a cabo efectivamente, vendrá a completar y concretar la información que ya se le había dado. Si la cesión no estuviera prevista en el momento inicial de la recogida de los datos, la necesidad de una información completa al titular de los datos resultaría más evidente.

Segundo, hay que tener en cuenta que la cesión de datos de carácter personal es una operación que abre la puerta a que una nueva persona, un tercero, cesionario, lleve a cabo un nuevo tratamiento de esos datos. Pues bien, el artículo 5 de la Ley que regula el derecho a ser informado, afecta a toda nueva manipulación de datos, también a la que derive de una cesión, y no sólo a la primera recogida. De esta manera, resulta perfectamente aplicable esta disposición concerniente a la información a los supuestos de cesión de datos. Parece lógico interpretar que si la cesión conlleva un nuevo tratamiento éste deberá hacerse con todas las garantías que exige la Ley al respecto, incluido el correcto y completo ejercicio del deber de informar. Y es que es difícil pensar que cuando se comunican los datos a una tercera persona el titular no tenga que ser informado sobre todos los puntos que reconoce esta última disposición: la identidad del destinatario, la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, etc.

En conclusión, se ha de entender que en la cesión la información tiene que ser completa, recogiendo todas las características que va a tener la nueva manipulación que el cesionario vaya a dar a dichos datos.

[2053] SAN 21 de septiembre de 2005, FJ 4, la citada señora no fue informada de que sus datos estaban siendo manipulados por la aseguradora de la parte contraria en un accidente. Evidentemente, la aseguradora que utilizaba la información debió informar a la titular de los datos.

En el ámbito sanitario, algunas normas de aplicación interna han recogido expresamente la necesidad de informar sobre la cesión o comunicación de los datos sanitarios. Con buen criterio, además, se ha reconocido la obligación de informar de una manera completa sobre las características de la cesión que se pretende. Es más, como ya ocurriera en la regulación del genérico derecho a la información, los puntos sobre los que se obliga a informar son más que los que se recogen en la regulación de la LOPD, siendo necesario facilitar los datos identificativos del responsable del fichero cedente: denominación, actividad, dirección postal, teléfono, y en su caso, fax y dirección de correo electrónico; los datos de carácter personal del interesado que obran en poder del responsable del fichero y cuya comunicación a un tercero se pretende autorizar; las circunstancias en que el responsable del fichero obtuvo los datos que se pretende comunicar, con mención de la información o consentimiento prestados con ocasión de la recogida de los mismos; la finalidad a la que se destinarán los datos cuya comunicación se pretende autorizar; la sujeción del cesionario, por el sólo hecho de la comunicación de los datos personales, a las disposiciones de la Ley Orgánica de Protección de Datos de Carácter Personal, 15/1999 de 13 de diciembre; la advertencia, gráficamente destacada, de que si no manifiesta lo contrario en el término de 15 días naturales contados a partir del día siguiente al de la recepción del comunicado, se entenderá que presta su consentimiento a la comunicación de sus datos personales expuesta[2054]. Se entiende aquí que siempre es preferible un exceso de información a una carencia de la misma. Más aún en un ámbito como el sanitario, donde la información constituye un elemento indispensable para la construcción de la necesaria relación de confianza entre médico y paciente.

Más allá de su contenido, el derecho a la información plantea algún otro problema de interpretación. Cabe preguntarse si es de aplicación directa el artículo 5.4 de la Ley a las cesiones de datos. Esta disposición señala que en los casos en que los datos no son recabados del propio afectado la información podrá dársele a éste en los tres meses siguientes al momento del registro de los datos. Podría entenderse que las cesiones son supuestos en que los datos no son recabados directamente del propio titular y que, por lo tanto, esta regulación es aquí aplicable. Así, hay autores que sin mayores matices han entendido que el deber de informar, cuando se trata de llevar adelante una cesión de datos, puede ser prorrogado durante tres meses[2055]. Es decir, la transmisión se realizaría sin que se informara al titular de los datos desde un inicio sobre este hecho. La información se llevaría a cabo durante los tres meses siguientes a producirse la cesión.

Esta interpretación, como se subrayó al analizar el derecho a ser informado, plantea serios problemas ya que podría llevar a entender que, al igual que la información, es posible también

[2054] Punto 8.6 Código Tipo de la Agrupación Catalana de Establecimientos Sanitarios, inscrito el 28 de diciembre del 2001; Artículo 10.1b), Código Tipo de la Unió Catalana de Hospitals, inscrito el 12 de julio de 2002 (modificado en julio de 2004).

[2055] MIRALLES MIRAVET y BACHES OPI, "La Cesión...", cit., 2001, el "art. 5.4 regula con carácter general y, por consiguiente, abarca también los supuestos de cesión, aquellas situaciones en las que los datos personales han sido obtenidos de una fuente distinta al interesado. El mencionado artículo impone una obligación de información al responsable de los datos dentro de los tres meses siguientes a la obtención de dichos datos, salvo que el interesado hubiese sido informado con anterioridad a la obtención de los datos de aquellos extremos a los que se refiere el precepto".

prorrogar el consentimiento. Hay que tener en cuenta que no hay consentimiento sin información. No se puede autorizar lo desconocido. No tiene sentido otorgar primero el consentimiento e informar después sobre lo que se ha autorizado. Siendo esto así, si se admitiera que la información es prorrogable también se admitiría la prórroga del consentimiento. Partiendo de esta base, si se entendiera que el citado precepto es aplicable a las cesiones de datos la conclusión a extraer resultaría nefasta. Si en todas las cesiones, en la medida en que son supuestos en que los datos no se recaban del propio titular, se pudiera prorrogar la información, se podría llegar a la conclusión de que en toda cesión de datos el consentimiento puede también prorrogarse junto con la información. Así, se abriría la puerta a la posibilidad de que las comunicaciones se lleven a cabo sin el previo consentimiento informado del titular, pues tanto el consentimiento como la información se podrían prorrogar. Es más, el régimen general para las cesiones podría ser ese, pues el artículo 5.4 tiene aplicación genérica a todos los casos en que los datos no se recaban del titular.

Lógicamente, esta interpretación carece de fundamento. La citada disposición fue analizada más arriba, bastando con hacer en este momento una remisión a lo dicho entonces. En todo caso, la crítica a dicha interpretación puede basarse en dos argumentos. Primero, la posibilidad de prorrogar la información no puede darse siempre que haya una cesión. Evidentemente, una tal prórroga deberá estar justificada. Se entendía al analizar el derecho a ser informado que la aplicación del artículo que ahora se comenta sólo tiene cabida cuando se refiere a supuestos en que el consentimiento está excepcionado, pero no así el deber de informar. Las causas que justifican una excepción al consentimiento pueden justificar el retraso en la información. Así, el deber de informar podría prorrogarse cuando el derecho del titular de los datos a consentir la cesión está limitado. Se salvaría, así, el problema de que la prórroga del deber de informar conlleve también la prórroga del deber de recabar el consentimiento. Segundo, hay que tener en cuenta que la interpretación que ahora se critica, en la medida en que posibilita la prórroga del derecho a consentir la transmisión de datos, iría en contra de la exigencia de que el consentimiento sea siempre previo al ejercicio de la comunicación, ya comentada. Si la autorización ha de ser previa a la operación carece de justificación admitir que se pueda prorrogar en el tiempo.

I.4.3. El principio de finalidad.

Como último requisito exige la Ley que la finalidad de la cesión esté directamente vinculada con las funciones legítimas del cedente y del cesionario[2056]. De la redacción de la norma se deduce que simplemente se requiere que en las comunicaciones los datos se destinen a fines relacionados con las funciones del cesionario y del cedente. No es necesario que las finalidades de ambos sujetos sean las mismas, ni siquiera que sean compatibles. Esta regulación plantea un problema interpretativo.

Al analizar el principio de finalidad se vio que la Ley dispone que los datos no podrán usarse para finalidades incompatibles con las que motivaron su recogida. Atendiendo a este último criterio lo lógico sería pensar, debido a que la cesión se integra dentro del concepto de

[2056] Artículo 11.1 LOPD.

tratamiento, que los datos sólo pueden cederse para el cumplimiento de una finalidad del cesionario compatible con la finalidad del cedente. El cesionario sólo podría manipular los datos si sus fines fueran compatibles con los que motivaron la recogida inicial de los datos. De la Directiva europea también podría desprenderse esta exigencia[2057]. Este criterio, sin embargo, no se sigue en la regulación estatal de la cesión. De la LOPD se desprende que basta con que la finalidad del nuevo tratamiento que llevará a cabo el cesionario sea acorde con sus funciones, funciones que tendrán una finalidad compatible o no con la finalidad del tratamiento realizado en inicio por el cedente[2058].

Esta regulación ha sido especialmente criticada por algunos autores[2059], que han justificado la aplicación directa del artículo 4 de la Ley al supuesto de la cesión[2060]. Según su criterio, los fines a seguir por el cesionario deberán ser compatibles con los perseguidos por el cedente. Se entiende aquí que estas críticas no son del todo afortunadas.

Hay que tener en cuenta que la cesión de datos lleva a un nuevo tratamiento. Además habrá que atender al hecho de que esta nueva manipulación se va a desarrollar también con todas las garantías previstas por la Ley: consentimiento e información fundamentalmente. Estas circunstancias hacen que la cesión pueda dedicarse a una finalidad distinta, e incluso incompatible, a la que llevó al cedente a la manipulación de datos. Se entiende que existen las garantías suficientes como para que puedan cederse los datos en orden a llevar a cabo una finalidad incompatible con la que motivó la recogida de datos por el cedente. Sin embargo, obviamente, el cesionario deberá respetar en todo caso el principio de finalidad, sin que pueda utilizar la información que recaba para otro fin que no sea el que motivó la cesión[2061].

Es posible, por lo tanto, salvar la aplicación de dicho artículo 4 para los casos de la cesión, de forma que no es necesario que los fines a seguir por cedente y cesionario sean compatibles. Puede hacerse, incluso, una interpretación más laxa a la que se acaba de indicar. La Ley exige que la cesión se dé para el cumplimiento de fines directamente relacionados con las funciones del cedente y del cesionario. Pues bien, una línea doctrinal ha entendido que a través del

[2057] Considerando nº 28 Directiva 95/46/CE: "*los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originalmente especificados*".

[2058] HERRÁN ORTIZ, *El Derecho…,* cit., 2002, p. 233: "puede concluirse que en la operación de cesión el legislador ha creído oportuno establecer una excepción en cuanto al principio de finalidad ya que en ningún caso exige que ésta deba producirse de acuerdo a los fines que no sean incompatibles, tal y como con carácter general se establece en el principio de finalidad, bien al contrario, será suficiente que la cesión responda directamente a las funciones del cedente y del cesionario, que no tienen que ser iguales, y ni tan siquiera compatibles".

[2059] HEREDERO HIGUERAS, *La Ley...,* cit., 1996, p. 117, por ejemplo, entiende que "si la cesión es parte del tratamiento (art. 3,c), sólo debería ser lícito ceder datos para la misma finalidad para la que los datos hubieran sido recogidos". HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 232, señala que en la cesión "la primera quiebra que se observa es la relativa al principio de finalidad ya que (...) el legislador no respeta ni se sujeta al principio general de finalidad"

[2060] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, pp. 100-101, afirma que la exigencia de la Directiva y la inclusión de la cesión dentro de la definición del concepto de tratamiento, son argumento suficiente para la aplicación del artículo 4º, que se aplica a todo tratamiento, a los supuestos de cesión.

[2061] Artículo 3.3 Orden de 20 de enero de 1995 del Consejero de Sanidad, por la que se regulan los Ficheros Automatizados de Datos de Carácter Personal gestionados por el Departamento de Sanidad y por Osakidetza-Servicio Vasco de la Salud: el "*responsable del fichero automatizado advertirá expresamente al cesionario de su obligación de dedicarlos exclusivamente para la finalidad para la que se ceden, de acuerdo con lo establecido en el artículo 11.5 en relación con el 4.2 de la misma Ley Orgánica".*

consentimiento del titular de los datos se puede justificar un tratamiento que no esté vinculado a las funciones del cedente o del cesionario. Se ha afirmado que el consentimiento debe ser suficiente para dar validez un tratamiento que nada tenga que ver con las citadas funciones[2062]. Basta la autorización de dicho titular para que se entienda que el cesionario puede manipular los datos con finalidades distintas a las marcadas por sus funciones.

Se está de acuerdo con esta interpretación. Siempre que el titular de los datos dé su consentimiento, fundamentado en una información sólida sobre lo que se va a hacer con sus datos, la cesión estará legitimada. En conclusión, el principio de finalidad debe entenderse aquí de forma flexible, de tal manera que se dé mayor margen de actuación a la voluntad del titular de los datos, sin que las características de la finalidad a perseguir condicionen la posibilidad de transmitir los datos.

I.4.4. Una referencia a la interpretación que los tribunales han hecho sobre un supuesto de incumplimiento de estos requisitos.

Las cesiones de datos de carácter personal han de cumplir, salvo causa que justifique lo contrario, los requisitos que se acaban de citar. Su incumplimiento invalidará de inicio la operación y será motivo para sancionar al cedente. A esta previsión lógica, sin embargo, ha de hacérsele un pequeño apunte.

Los tribunales han señalado que si se da una comunicación de datos defectuosa a un cesionario que ya tenía la información que se le transmite, a pesar de los defectos que pueda tener la operación, el cedente que ha cometido la irregularidad no podrá ser sancionado[2063]. A pesar de no cumplir los requisitos citados, en estos casos no se sancionará al cedente. Lo mismo ocurre cuando se revelan datos que ya eran públicos[2064]. Se interpreta que, en la medida en que el cesionario ya tenía conocimiento de la información, difícilmente puede considerarse que la transmisión de los datos, aunque realizada de manera irregular, sin la obtención del consentimiento por ejemplo, pueda causar daño alguno al afectado, por lo que no puede entenderse dicha acción como sancionable.

Si bien la decisión aportada por la jurisprudencia puede ser acertada desde el punto de vista del Derecho sancionador, desde un punto de vista conceptual no puede admitirse que el hecho de que el cesionario ya cuente con los datos lleve a una situación en que dichas operaciones no sean fiscalizables. Hay que tener en cuenta que esa transmisión, a pesar de que el cesionario ya conozca los datos, puede plantear nuevos riesgos. No hay que olvidar el hecho de que toda comunicación constituye un peligro en sí misma, en la medida en que facilita el que los datos se puedan sustraer, perder o alterar. Será necesario analizar cada supuesto para poder llegar a la conclusión a la que, de manera genérica, han llegado los tribunales.

[2062] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 159; BUISÁN GARCÍA, "Comunicación de datos…", cit., 2008, p. 290.
[2063] SSAN 22 de septiembre 2004, FJ 4; 7 de noviembre 2007, FJ 5.
[2064] Resolución APDCM, 17 de septiembre de 2009, "La difusión de un dato personal ya conocido públicamente no vulnera el artículo 10 de la LOPD".

I.5. Excepciones al consentimiento en la cesión de datos.

El punto de partida a la hora de ceder los datos sanitarios ha de ser el requerimiento del consentimiento del titular de los datos. Respetar, de inicio, el derecho de cada uno a autorizar toda comunicación de los datos que se refieren a su persona constituye una premisa fundamental a guardar por los responsables de los ficheros. La excepción a este derecho a consentir deberá estar justificada en cada caso[2065].

El incumplimiento de esta regla conlleva sanción[2066]. Es más, como se apuntara más arriba, comunicar o revelar esta información sin la autorización requerida puede llegar a constituir un delito[2067]. Además, en lo que en este trabajo se analiza, se trataría de un delito especialmente grave. En primer lugar por la agravante que supone que la cesión se lleve a cabo por el propio profesional de la sanidad[2068]. Y en segundo lugar porque se trata de ceder datos sensibles, como son los relativos a la salud[2069]. No hay que olvidar que los datos relativos a la salud de las personas son considerados por la propia Ley como especialmente protegidos[2070].

Tanto la normativa de protección de datos como la sanitaria reconocen una serie de supuestos en que no es necesario el consentimiento del titular para llevar a cabo la cesión. Ambos ordenamientos deberán interpretarse conjuntamente. Hay que recordar, que las excepciones que ahora se verán justifican también la vulneración del deber de secreto.

I.5.1. Excepción al consentimiento en la cesión de datos por determinación de una Ley.

I.5.1.A. Requisitos que ha de cumplir la Ley para aplicar la excepción.

Según la LOPD no se requiere el consentimiento del titular de los datos para llevar a cabo una cesión cuando ésta "*está autorizada en una ley*"[2071]. El Reglamento que desarrolla la Ley concreta esta excepción[2072]. La Directiva no hace mención expresa a este respecto. La

[2065] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, p. 41.
[2066] Artículo 44.4.b) LOPD.
[2067] SAN 12 de abril de 2002; AAP de Madrid, 19 de octubre de 2004, FJ 3.
[2068] GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 344: en relación al art. 197.4: cualificación por la condición del sujeto activo de responsable o encargado de los ficheros, soportes, archivos o registros del sujeto activo. "La persona encargada o responsable ocupa una posición especial y privilegiada de garante por ley o contrato de los soportes de los secretos, cuyo conocimiento por parte de terceros se intenta evitar. Ello le sitúa en una posición privilegiada para vulnerar el bien jurídico protegido, lo cual se ha tenido en cuenta para la cualificación establecida".
[2069] GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 371: en relación al art. 197.5: "La razón de la agravación prevista en el apartado 5 del art. 197 CP se encuentra en la mayor antijuridicidad de la conducta, que se manifiesta, por un lado, en la lesión de lo que se ha dado en denominar el <<núcleo duro de la "privacy">> (la esfera más sensible de la misma), en el caso del primer inciso del art. 197.5 CP".
p. 373: "Los datos protegidos en el apartado 5 del art. 197 CP son los que el art. 7 LOPD denomina datos especialmente protegidos, es decir, aquellos que (p. 374) revelan la ideología, religión, creencias, salud, origen racial o vida sexual".
[2070] Artículo 7.3 LOPD. GRACIA GUILLÉN, "La Confidencialidad…", cit., 2000, pp. 30-31.
[2071] Artículo 11.2.a) LOPD.
[2072] Artículo 10.2 RDLOPD: "*No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando: a) Lo autorice una norma con rango de ley o una norma comunitaria y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tenga por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalzca el interés o los derechos y libertades fundamentales de los interesados previstos en*

Recomendación del Consejo de Europa que regula la protección de datos médicos, por su parte, reconoce la posibilidad de comunicar datos de salud sin el consentimiento del titular, cuando lo prevea una Ley, siempre que esta previsión legal responda a unos motivos determinados[2073].

En diferentes ámbitos pueden encontrarse leyes que reconocen la necesidad de que datos de carácter personal sean cedidos entre diferentes sujetos[2074]. En materia de tráfico, por ejemplo, las normas han dispuesto el deber de ceder datos de personas implicadas en un accidente sin necesidad de su consentimiento. La finalidad de esta comunicación es la de suministrar la información pertinente para que esas personas puedan averiguar, a la mayor brevedad posible, los datos relativos a la entidad aseguradora que cubre la responsabilidad civil de los vehículos implicados en el accidente y facilitar el control de la obligación de asegurarse[2075]. En otro ámbito

---

el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre. El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento un deber que le imponga una de dichas normas".

[2073] Artículo 7.3 R (97) 5: "*Los datos médicos pueden comunicarse si son relevantes y:*
a)si la comunicación está prevista por la ley y constituye una medida necesaria en una sociedad democrática por: i. razones de salud pública; ii. La prevención de un peligro real o la represión de un delito específico; iii. otro interés público importante; iv. La protección de los derechos y las libertades de otros".

[2074] TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 964, apunta algunos supuestos en que la Ley exceptúa el consentimiento.

[2075] Artículo 23 Real Decreto 1507/2008, 12 de septiembre de 2008, por el que se aprueba el Reglamento del Seguro Obligatorio de Responsabilidad Civil: *"1. Las entidades aseguradoras que cubran mediante el seguro obligatorio la responsabilidad civil derivada de la circulación de vehículos a motor con estacionamiento habitual en España, deberán comunicar al Ministerio de Economía y Hacienda, mediante su remisión al Consorcio de Compensación de Seguros, los datos relativos a los vehículos asegurados por ellas, así como los relativos al representante para la tramitación y liquidación de siniestros designado por la entidad aseguradora en cada uno de los Estados del Espacio Económico Europeo, con el contenido, la forma y en los plazos que se establecen en este reglamento y en las resoluciones a que éste se refiere (...).2. Los datos a que se refiere el apartado anterior serán objeto de tratamiento automatizado mediante el fichero automatizado de datos de carácter personal, denominado Fichero Informativo de Vehículos Asegurados, de carácter público, regulado en este Reglamento, con el contenido que se describe en los artículos siguientes y en el anexo"*; Artículo 24: *"1. En la primera remisión de los datos, las entidades aseguradoras suministrarán, por cada vehículo, los siguientes: matrícula, código identificativo de la marca y modelo del vehículo, fecha de inicio de la vigencia y fecha de finalización del período de seguro en curso, así como el tipo de contrato, todo ello de acuerdo con las especificaciones contenidas en la resolución de la Dirección General de Seguros y Fondos de Pensiones dictada a tal efecto. Asimismo, deberá remitirse el nombre y dirección del representante para la tramitación y liquidación de siniestros designado por la entidad aseguradora en cada uno de los Estados del Espacio Económico Europeo. 2. Por las entidades aseguradoras se realizará la actualización de datos, remitiendo diariamente información de altas y bajas de vehículos asegurados, que se identificarán con su matrícula y código identificativo de su marca y modelo, haciendo constar, en el caso de altas, las fechas de inicio de la vigencia y finalización del período de seguro en curso, tipo de contrato y, en caso de bajas, la fecha de cese de la vigencia del seguro (...)"*; Artículo 27: *"1. A efectos de acceso al fichero, tienen la consideración de implicados los perjudicados por accidentes de circulación, por daños en su persona o en sus bienes, pudiendo actuar por sí o por medio de representante debidamente acreditado. 3. A efectos de lo dispuesto en el apartado 2 del artículo 25 del texto refundido de la Ley sobre responsabilidad civil y seguro en la circulación de vehículos a motor, se considera que existe interés legítimo del perjudicado en obtener información sobre la identidad del propietario, conductor o titular del vehículo en el supuesto de que para el total resarcimiento de los daños sólo pueda reclamarse contra esas personas*"; Artículo 28: *"El control de la obligación de asegurarse se realizará mediante la colaboración entre el Ministerio de Economía y Hacienda, a través del Consorcio de Compensación de Seguros, y el Ministerio del Interior, a través de la Dirección General de Tráfico, que podrán cederse, entre sí, los datos que figuren en sus ficheros automatizados que expresamente prevean esta cesión.*
El procedimiento de cesión de datos se regulará mediante resolución conjunta de la Dirección General de Seguros y Fondos de Pensiones y de la Dirección General de Tráfico.
*El órgano responsable del fichero adoptará las medidas técnicas y organizativas que sean necesarias para asegurar la confidencialidad, seguridad e integridad de los datos y hacer efectivas las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal"***.** Artículo 25.2 RDL 8/2004, 29 de octubre de 2004, por el que se aprueba el Texto Refundido de la Ley sobre

como el de la investigación policial también se encuentran normas que prevén la posibilidad de llevar a cabo cesiones de datos de carácter personal entre diferentes entidades. La finalidad en este caso es la prevención y persecución de los delitos[2076]. Lo mismo ocurre en el ámbito tributario, donde se reconocen diferentes supuestos en que la transmisión de información relativa a personas está permitida, sin necesidad de que se requiera el consentimiento del titular[2077].

La excepción que ahora se analiza deriva de la genérica regulación que la Ley realiza sobre el consentimiento para el tratamiento común de los datos de carácter personal. Se señala en la norma que la manipulación de esta información requerirá de la autorización del titular, salvo que la ley disponga otra cosa[2078]. Pueden trasladarse a este punto las consideraciones que se realizaron en el apartado dedicado a analizar el derecho al consentimiento en relación a esta excepción[2079], sobre todo, lo dicho sobre el rango que debe tener la norma que establece el límite. Sin embargo, han de realizarse una serie de apuntes concretos sobre este precepto concerniente a la cesión.

A) En primer lugar, cabe preguntarse si para que quepa la excepción basta con que la Ley prevea la cesión o si es necesario que el legislador establezca expresamente que queda

---

Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor: *"El Consorcio de Compensación de Seguros facilitará, asimismo, al perjudicado el nombre y la dirección del propietario, del conductor habitual o del titular legal del vehículo con estacionamiento habitual en España, si aquel tuviera un interés legítimo en obtener dicha información. A estos efectos, la Dirección General de Tráfico o la entidad aseguradora proporcionará estos datos al Consorcio de Compensación de Seguros, y se establecerán, en todo caso, las medidas técnicas y organizativas necesarias para asegurar la confidencialidad, seguridad e integridad de los datos y las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A la información de que disponga el Consorcio de Compensación de Seguros tendrán acceso, además de los perjudicados, los aseguradores de éstos, los organismos de información de otros Estados miembros del Espacio Económico Europeo, la Oficina Española de Aseguradores de Automóviles, en su calidad de organismo de indemnización, y los organismos de indemnización de otros Estados miembros del Espacio Económico Europeo, así como los fondos de garantía de otros Estados miembros del Espacio Económico Europeo. Tendrán también acceso a dicha información los centros sanitarios y servicios de emergencias médicas que suscriban convenios con el Consorcio de Compensación de Seguros y las entidades aseguradoras para la asistencia a lesionados de tráfico".*

[2076] Artículo 7 LO 10/2007, 8 de octubre, reguladora de la Base de Datos Policial sobre Identificadores obtenidos a partir del ADN: "*Podrán cederse los datos contenidos en la base de datos: a) A las Autoridades Judiciales, Fiscales o Policiales de terceros países de acuerdo con lo previsto en los convenios internacionales ratificados por España y que estén vigentes; b) A las Policías Autonómicas con competencia estatutaria para la protección de personas y bienes y para el mantenimiento de la seguridad pública (...); c) Al Centro Nacional de Inteligencia, que podrá utilizar los datos para el cumplimiento de sus funciones relativas a la prevención de tales delitos (...)*".

[2077] Artículo 95 Ley 58/2003, de 17 de diciembre, General Tributaria: "*1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto: a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada; b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias; c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social, así como en la obtención y disfrute de prestaciones a cargo de dicho sistema; d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea. e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido. (...)*". DELGADO GARCÍA y OLIVER CUELLO, *Administración Electrónica Tributaria…,* cit., 2009, p. 37.

[2078] Artículo 6.1 LOPD.

[2079] TRONCOSO REIGADA, *Protección de Datos…*, cit., 2008, p. 77.

exceptuado el consentimiento para dicha comunicación. De la LOPD podría desprenderse la idea de que, para que se entienda que la excepción es aplicable se requiere la previsión expresa y concreta de que no hay que recabar el consentimiento para una cesión determinada[2080]. En su articulado, en relación a la modificación de la Ley General Tributaria, dispone expresamente que no será necesario el consentimiento para comunicar los datos pertinentes a la Administración tributaria[2081]. Se podría entender, que en la medida en que la LOPD adopta el criterio de fijar expresamente la excepción al consentimiento, esta fórmula será la que deberán seguir todas las normas que quieran prever una cesión de datos sin autorización del titular de los mismos. La doctrina ha mostrado ciertas dudas a la hora de dar solución a esta cuestión[2082].

A pesar de lo dispuesto en la LOPD, parece que la interpretación que ha prevalecido en la práctica ha sido la que entiende que la simple previsión por una norma de rango legal de una cesión puede conllevar la excepción del consentimiento[2083]. La norma no tendría que reconocer expresamente que no es necesaria la autorización. Es decir, bastaría que una Ley dispusiera una cesión de datos para que no fuera imprescindible recabar el consentimiento del titular.

Realmente no es muy afortunado, teniendo en cuenta que se trata de limitar un derecho fundamental, que la excepción al consentimiento pueda establecerse de manera tan ambigua. El límite al derecho fundamental debería recogerse de forma expresa. Lo contrario podría llevar a que la regla general fuera la excepción en vez de la vigencia del derecho. Si se entiende que el mero hecho de que una Ley recoja una cesión conlleva la excepción al consentimiento, puede interpretarse *a sensu contrario* que para que el derecho a consentir tenga aplicación y vigencia será necesario que esté recogido de manera expresa en la Ley. Y es que si la Ley no dice nada al respecto, y simplemente prevé la existencia de la cesión, se interpretará que el derecho a consentir queda limitado. El silencio jugaría a favor de la excepción en detrimento del derecho a la autodeterminación informativa del afectado.

Se entiende aquí que la excepción, si bien no exige una declaración expresa por parte del legislador eximiendo al responsable del fichero de la obligación de recabar dicha autorización, sí requiere el empleo de términos que sugieran la obligatoriedad de llevar a cabo la cesión. La utilización de verbos como "transmitirán" o "comunicarán", o "deberán" o "tendrán", haciendo referencia a la comunicación de datos, pueden llevar a entender que la cesión es obligatoria y que no se requiere el consentimiento del titular para realizarla. Estas expresiones son empleadas, por ejemplo, en los casos que se han citado sobre las cesiones de datos con fines

[2080] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 161.

[2081] DA Cuarta LOPD: "*Modificación del artículo 112.4 de la Ley General Tributaria.- El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:*
<<4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal".

[2082] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión…,* cit., 2003, pp. 110-113.

[2083] BUISÁN GARCÍA, *"*Comunicación de datos…", cit., 2008, p. 301; TRONOOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 967: en relación a las cesiones a las administraciones públicas, señala que "Basta con que la ley establezca competencias administrativas para considerar como legítima la comunicación de la información para el cumplimiento".

policiales o de control del cumplimiento de la obligación de asegurarse[2084]. No parece que el mero hecho de que una norma con rango legal recoja una cesión de datos pueda conllevar automáticamente la excepción del consentimiento. Lo que limitará el derecho a la autodeterminación informativa del titular de los datos será el que la citada Ley obligue a llevar a cabo dicha cesión. Esta interpretación se encontraría en la línea establecida por el nuevo reglamento que desarrolla la LOPD, que dispone que el consentimiento no será necesario para la realización de una cesión cuando esta operación constituya un deber "impuesto" por las leyes[2085].

B) En segundo lugar, como ya se dijera en el apartado relativo al consentimiento, para aplicar la excepción que se analiza no basta con que una Ley la prevea. Será necesario además que la regulación se dirija a proteger un bien jurídico de suficiente entidad[2086]. La recomendación del Consejo de Europa que regula la protección de datos médicos así parece haberlo entendido: no es suficiente con la previsión legal, sino que es necesario que la Ley se fundamente en un argumento sólido para que la cesión sin la concurrencia del consentimiento del titular de los datos sea legítima[2087]. En este sentido, el RDLOPD dispone que la excepción al consentimiento tendrá justificación cuando la cesión se dirija a satisfacer un interés "legítimo" del responsable o cesionario y no prevalezca un interés, un derecho o una libertad del titular de los datos[2088]. El reglamento exige que la justificación del límite al derecho a consentir por previsión legal ha de resultar de la ponderación de los bienes jurídicos que puedan entrar en conflicto en cada comunicación.

Cierto es que en la mayoría de casos los intereses que justifican la excepción que se analiza aparecen descritos empleando conceptos indeterminados, que no ayudan a garantizar la seguridad jurídica. Es lo que ocurre, por ejemplo, con el concepto de "*otro interés público*", empleado en la citada recomendación. Estas previsiones podrían entenderse contrarias a la ya conocida exigencia de que será necesario que la norma de rango legal que excepcione el consentimiento sea concreta y fije la excepción de forma inequívoca y expresa. Es decir, los límites deberán estar dispuestos de tal manera que los titulares de los datos conozcan claramente cuándo se limita su derecho a controlar la información que les concierne. Fundamentalmente, la jurisprudencia del TEDH ha establecido la necesidad de que todo límite al derecho del que aquí se habla cumpla los requisitos que garanticen la seguridad jurídica de los ciudadanos[2089]. A pesar de ello, se entiende que los matices que aporta la recomendación deben ser tenidos en cuenta en el ámbito estatal. Hay que entender, en conclusión, que cuando se reconoce la posibilidad de que una Ley excepcione la facultad del titular de unos datos de otorgar el consentimiento para autorizar una cesión, será necesario que esa Ley se fundamente en un interés digno de protección. El principio de proporcionalidad así lo exige también.

[2084] Se podría citar, también, el artículo 53.2 Ley 29/2006, 26 de julio, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios: "*Los profesionales sanitarios tienen el deber de comunicar con celeridad a los órganos competentes en materia de farmacovigilancia de cada Comunidad Autónoma las sospechas de reacciones adversas de las que tengan conocimiento y que pudieran haber sido causadas por medicamentos*". SAN 24 octubre 2007, FJ 4.

[2085] Artículo 10.2.a) RDLOPD.

[2086] GUICHOT, *Datos Personales…,* cit., 2005, p. 255.

[2087] Artículo 7.3 R (97) 5.

[2088] Artículo 10.2.a) RDLOPD.

[2089] SSTEDH, 4 de mayo del 2000, Rotaru v. Rumanía, apdo. 52; 23 de septiembre de 2008, Reyhan v. Turquía, FJ 23.

I.5.1.B. La aplicación de la excepción en el ámbito sanitario.

La aplicabilidad de la excepción que se está analizando al ámbito sanitario no se deduce sólo de la LOPD, sino que se reconoce expresamente en la LBAP[2090]. En este sector pueden encontrarse supuestos en que normas con rango legal establecen la obligación de llevar a cabo cesiones de datos relativos a la salud de las personas. No es necesario tratar de reconocer todos los casos en que las leyes disponen la obligación de realizar cesiones de datos en el ámbito sanitario. Bastará con dar unos ejemplos para poder identificar cuándo se exceptúa la necesidad de recabar el consentimiento en este ámbito.

La mayoría de las leyes que se citarán a continuación cuentan con rango de Ley ordinaria. Esta circunstancia podría plantear algún problema desde el punto de vista de la teoría general sobre los derechos fundamentales. Como se dijera más arriba, los límites a los derechos fundamentales han de ser fijados de inicio, según jurisprudencia del TC ya citada, por leyes orgánicas, que son objeto de un mayor consenso en sede parlamentaria. El hecho de que sean leyes ordinarias las que establezcan estas excepciones puede justificarse por el hecho de que las leyes que entran en el ámbito sanitario a exceptuar el derecho a autorizar las cesiones de datos cuentan con la cobertura de la LOPD. Por un lado, esta norma habilita al legislador para establecer estas excepciones. Y por otro, da cobertura a todas las leyes que exceptúan el consentimiento en tratamientos de datos dirigidos a la protección de la salud de las personas. En la medida en que la propia Ley justifica las cesiones con dicho fin, las demás leyes ordinarias que prevean otras comunicaciones en sectores específicos de la sanidad no serán más que la concreción de la propia Ley orgánica.

Pueden exponerse diferentes ejemplos en que se aplica esta excepción. En el ámbito puramente sanitario la Ley de Cohesión y Calidad del Sistema Nacional de Salud establece supuestos en que el derecho a consentir la cesión de datos queda exceptuado, por estar el tratamiento dirigido a proteger la salud de las personas[2091]. En este caso, la excepción viene refrendada por el nuevo reglamento de desarrollo de la LOPD, que recoge de manera expresa que las cesiones reconocidas en la Ley de Cohesión y Calidad del Sistema Nacional de Salud no requieren la autorización del titular de los datos[2092].

[2090] Artículo 7.1 LBAP: "*Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a la salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley*"

[2091] Artículo 53 Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: " *1. El Ministerio de Sanidad y Consumo establecerá un sistema de información sanitaria del Sistema Nacional de Salud que garantice la disponibilidad de la información y la comunicación recíprocas entre las Administraciones sanitarias. Para ello en el seno del Consejo Interterritorial del Sistema Nacional de Salud se acordarán los objetivos y contenidos de la información (...)*

5. Las comunidades autónomas, la Administración General del Estado y las Entidades Gestoras de la Seguridad Social aportarán a este sistema de información sanitaria los datos necesarios para su mantenimiento y desarrollo. Del mismo modo, las Administraciones autonómicas y estatal tienen derecho de acceder y disponer de los datos que formen parte del sistema de información que precisen para el ejercicio de sus competencias.

6. La cesión de los datos, incluidos aquellos de carácter personal necesarios para el sistema de información sanitaria, estará sujeta a la legislación en materia de protección de datos de carácter personal y a las condiciones acordadas en el Consejo Interterritorial del Sistema Nacional de Salud".

[2092] Artículo 10.5 RDLOPD: "*Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.*

En esta Ley, siguiendo el principio que exige colaboración entre administraciones[2093], se establece la necesidad de transmitir datos entre diferentes entidades con la finalidad de mejorar el sistema de protección de la salud de los ciudadanos, en todas sus vertientes. Esta transmisión se puede dar entre centros sanitarios, Administración autonómica y Administración estatal. El intercambio de datos de salud por medios telemáticos aparece en esta norma con rango legal como una operación necesaria y obligatoria para prestar un servicio de calidad[2094], dirigido, sobre todo, a que cualquier ciudadano pueda ser atendido en cualquier momento en cualquier punto del territorio estatal. Esta previsión legal lleva a que las cesiones de datos que se vayan a dar en la práctica no tengan que contar con el consentimiento de cada afectado. El empleo en esta norma de verbos como "aportarán" o "establecerá" deja entrever la pertinencia de la excepción y la obligatoriedad de la cesión.

En la medida en que las comunicaciones de datos se llevarán a cabo en este caso por prescripción legal, y teniendo en cuenta los riesgos que este tipo de operaciones generan, la propia Ley hace hincapié en la necesidad de adoptar las medidas de seguridad necesarias para que se realicen con todas las garantías precisas. El cumplimiento de las medidas de seguridad previstas por la LOPD para los ficheros que contienen datos sensibles es un primer paso. No obstante, a estas medidas se suman la creación del Instituto de Información Sanitaria como órgano que velará por el buen funcionamiento del sistema de información[2095], y de manera especial la necesidad de transmitir los datos de acuerdo con los parámetros de utilización de la firma electrónica[2096].

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para al atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud".

[2093] Artículo 2 LPAC: "*Las Administraciones públicas, en sus relaciones, se rigen por el principio de cooperación y colaboración".*

[2094] Artículo 56 Ley 16/2003, de 28 de mayo de Cohesión y Calidad del Sistema Nacional de Salud: "*Intercambio de información en salud entre organismos, centros y servicios del Sistema Nacional de Salud.*

Con el fin de que los ciudadanos reciban la mejor atención sanitaria posible en cualquier centro o servicio del Sistema Nacional de Salud, el Ministerio de Sanidad y Consumo coordinará los mecanismos de intercambio electrónico de información clínica y de salud individual, previamente acordados con las comunidades autónomas, para permitir tanto al interesado como a los profesionales que participan en la asistencia sanitaria el acceso a la historia clínica en los términos estrictamente necesarios para garantizar la calidad de dicha asistencia y la confidencialidad e integridad de la información, cualquiera que fuese la Administración que la proporcione.

El Ministerio de Sanidad y Consumo establecerá un procedimiento que permita el intercambio telemático de la información que legalmente resulte exigible para el ejercicio de sus competencias por parte de las Administraciones públicas.

El intercambio de información al que se refieren los párrafos anteriores se realizará de acuerdo con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en la Ley 41/2002, de 14 de noviembre".

[2095] Artículo 58 Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud; Artículo 12.3.b) RD 1555/2004, 25 de junio, por el que se desarrolla la Estructura Orgánica Básica del Ministerio de Sanidad y Consumo.

[2096] Artículo 54 Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: "*Red de comunicaciones del Sistema Nacional de Salud.*

El Ministerio de Sanidad y Consumo, a través de la utilización preferente de las infraestructuras comunes de comunicaciones y servicios telemáticos de las Administraciones públicas, pondrá a disposición del Sistema Nacional de Salud una red segura de comunicaciones que facilite y dé garantías de protección al intercambio de información exclusivamente sanitaria entre sus integrantes.

En ámbitos más concretos de la sanidad, a los que también hace referencia expresa la Ley de Cohesión y Calidad, se identifican normas con rango legal que prevén el intercambio de datos como instrumento necesario para el desarrollo de distintas actividades. La Ley de Garantías y Uso racional de Medicamentos y Productos Sanitarios es un claro ejemplo. En primer lugar, establece una obligación genérica de transmitir información sanitaria entre diferentes instituciones, para que éstas puedan ejercer con efectividad sus competencias en cumplimiento de la propia Ley[2097]. Y después, se refiere a operaciones más concretas en las que también se estiman necesarias las comunicaciones. Es el caso de la farmacovigilancia. Señala la Ley de Garantías y Uso racional de Medicamentos y Productos Sanitarios que los profesionales médicos, al igual que los profesionales farmacéuticos, deberán transmitir al órgano competente en cada Comunidad Autónoma las sospechas de reacciones adversas de determinados medicamentos[2098]. Esta comunicación se llevará a cabo a través de un formulario en el que se incluirán diversos datos y que será remitida a la Unidad de Farmacovigilancia correspondiente[2099]. El intercambio de información en el ámbito de la farmacovigilancia se facilita desde las normas con la promoción de modelos tecnológicos compatibles, que favorecen precisamente el flujo de datos[2100].

En la CAPV la que se denomina Red de Alerta de Farmacovigilancia, que está formada por los profesionales sanitarios y los fabricantes y titulares de autorización para comercializar con medicamentos, deberá informar sobre las sospechas de reacciones adversas a cualquier medicamento a la Unidad de Farmacovigilancia. Tras la evaluación del riesgo este órgano transmitirá la información a la Dirección de Farmacia del Departamento de Sanidad[2101]. Después,

---

La transmisión de la información en esta red estará fundamentada en los requerimientos de certificación electrónica, firma electrónica y cifrado, de acuerdo con la legislación vigente.
A través de dicha red circulará información relativa al código de identificación personal único, las redes de alerta y emergencia sanitaria, el intercambio de información clínica y registros sanitarios, la receta electrónica y la información necesaria para la gestión del Fondo de cohesión sanitaria, así como aquella otra derivada de las necesidades de información sanitaria en el Sistema Nacional de Salud".

[2097] Artículo 5 Ley 29/2006, de 26 de julio, de Garantías y Uso racional de Medicamentos y Productos Sanitarios: "1. *A efectos de salvaguardar las exigencias de salud y seguridad pública, las Administraciones públicas están obligadas a comunicarse cuantos datos, actuaciones o informaciones se deriven del ejercicio de sus competencias y resulten necesarias para la correcta aplicación de esta Ley*". TRONCOSO REIGADA, *Protección de Datos…,* Cit,. 2008, pp. 116-117 y 120.

[2098] Artículo 53 Ley 29/2006, de 26 de julio, de Garantías y Uso racional de Medicamentos y Productos Sanitarios: "*2. Los profesionales sanitarios tienen el deber de comunicar con celeridad a los órganos competentes en materia de farmacovigilancia de cada Comunidad Autónoma las sospechas de reacciones adversas de las que tengan conocimiento y que pudieran haber sido causadas por medicamentos.*
3. Los titulares de la autorización también están obligados a comunicar a las autoridades sanitarias de las Comunidades Autónomas las sospechas de reacciones adversas de las que tengan conocimiento y que pudieran haber sido causadas por los medicamentos que fabrican o comercializan, de conformidad con las buenas prácticas de farmacovigilancia (...)".

[2099] http://www.osanet.euskadi.net/

[2100] Artículo 3.3 RD 1344/2007, 22 de octubre, por el que se regula la Farmacovigilancia de Medicamentos de Uso Humano: "*Para facilitar el intercambio de la información sobre casos individuales de sospechas de reacciones adversas, se aplicarán las directrices elaboradas y publicadas por la Comisión Europea en el Volumen 9A de las Normas sobre medicamentos en la Unión Europea, relativas a la recopilación, verificación y presentación de notificaciones de reacciones adversas, incluyendo los requisitos técnicos en materia de intercambio electrónico de información sobre farmacovigilancia, con arreglo a los formatos acordados internacionalmente y sobre la terminología médica internacionalmente aceptada*".

[2101] Decreto 239/2002, de 15 de octubre, por el que se regula el Sistema de Farmacovigilancia de la Comunidad Autónoma del País Vasco.

esta información será comunicada a su vez a la Agencia Española de Medicamentos y Productos Sanitarios[2102], para pasar en algunos casos a formar parte de otras redes europeas e internacionales de farmacovigilancia[2103].

Todas estas transmisiones constituyen cesiones de datos, que incluso pueden llegar a darse en el ámbito internacional. El hecho de que la Ley recoja como una operación necesaria estas cesiones y que su fundamento lo constituya la protección de la salud de los ciudadanos hace que el consentimiento del titular de los datos no sea necesario para llevar a cabo este tratamiento. En este caso la expresión que emplea la Ley es especialmente clarificadora al decir "tienen el deber de comunicar".

La transmisión de datos en el ámbito farmacéutico va más allá del concreto caso de la farmacovigilancia. La ya citada Ley de Cohesión y Calidad del Sistema Nacional de Salud reconoce la necesidad de comunicar datos entre oficinas de farmacia y el Sistema Nacional de Salud, para poder hacer efectiva la colaboración entre ambos con la finalidad principalmente de controlar el uso de medicamentos[2104]. Lo cierto es que en este último caso la Ley no habla expresamente de la necesidad de ceder datos de salud entre diferentes entidades. No obstante, la norma sí hace referencia a una necesaria colaboración entre instituciones. Esta circunstancia puede llevar a entender, sin forzar demasiado la letra de la Ley, que es necesario un flujo de información entre estas entidades, pues la colaboración necesariamente requerirá de transmisiones de información. La propia jurisprudencia se ha hecho eco de la obligación que imponen las leyes en estos supuestos de transmisión de información[2105].

En otras normas reguladoras de la materia sanitaria se pueden observar previsiones de similares características. En el ámbito autonómico se ha recogido, por ejemplo, la obligación de

[2102] Artículo 53.4 Ley 29/2006, de 26 de julio, de Garantías y Uso racional de Medicamentos y Productos Sanitarios.

[2103] Artículo 54.2 Ley 29/2006, de 26 de julio, de Garantías y Uso racional de Medicamentos y Productos Sanitarios; Artículo 5.1.f), RD 1344/2007, de 11 de octubre, por el que se regula la Farmacovigilancia. En el ámbito europeo la Directiva 2010/84/UE, 15 de diciembre, del Parlamento Europeo y del Consejo, que modifica, en lo que respecta a la farmacovigilancia, la Directiva 2001/83/CE 6 de noviembre de 2001, por la que se establece un Código Comunitario sobre Medicamentos para Uso Humano, recoge en su articulado diferentes situaciones en que se transmite información por redes europeas.

[2104] Artículo 33 Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: "*Colaboración de las oficinas de farmacia. 1. Las oficinas de farmacia colaborarán con el Sistema Nacional de Salud en el desempeño de la prestación farmacéutica a fin de garantizar el uso racional del medicamento. Para ello los farmacéuticos actuarán coordinadamente con los médicos y otros profesionales sanitarios.*

2. En el marco de la Ley 25/1990, de 20 de diciembre, del Medicamento, el Ministerio de Sanidad y Consumo, previo acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, establecerá los criterios generales y comunes para el desarrollo de la colaboración de las oficinas de farmacia, por medio de conciertos que garanticen a los ciudadanos la dispensación en condiciones de igualdad efectiva en todo el territorio nacional, independientemente de su comunidad autónoma de residencia.

Se tenderá a la dispensación individualizada de medicamentos y a la implantación de la receta electrónica, en cuyo desarrollo participarán las organizaciones colegiales médica y farmacéutica.

3. Entre los criterios del apartado anterior se definirán los datos básicos de farmacia, para la gestión por medios informáticos de la información necesaria para el desempeño de las actividades anteriormente mencionadas y para la colaboración con las estructuras asistenciales del Sistema Nacional de Salud. Se ajustarán a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y a las especificaciones establecidas por los servicios de salud de las comunidades autónomas".

[2105] SAN 24 de octubre de 2007, FJ 4, en el que se hace referencia a la Ley del Medicamento y a la normativa que la desarrolla, como marco que justifica la cesión sin consentimiento.

ceder datos sanitarios con el fin de crear un registro poblacional de cáncer. Expresamente se dispone que los centros "estarán obligados a suministrar" los datos para crear el citado registro[2106]. Esta redacción no parece dejar lugar a dudas sobre la posibilidad de ceder datos de carácter sanitario sin necesidad de recabar el consentimiento de los titulares.

Como se ha podido observar, en todas estas normas que se han citado se prevén de manera más o menos concreta cesiones de datos que no requerirán del consentimiento del titular. La mayoría de los supuestos planteados tienen por finalidad la prestación de un servicio sanitario eficiente dirigido a proteger la salud de las personas. Los ejemplos expuestos hasta ahora se limitan a recoger situaciones en que se transmiten los datos con el fin de proteger la salud de los ciudadanos. Sin embargo, el legislador ha previsto también supuestos en que la cesión se produce a favor de un sujeto situado fuera de dicho ámbito.

Claro ejemplo de este caso es lo que ocurre con el acceso de funcionarios de la Seguridad Social a información contenida en ficheros de la Administración sanitaria. Evidentemente, el control por parte de la Seguridad Social de las diferentes contingencias que pueden darse en el desarrollo de la vida laboral de una persona, que tienen que ver con su estado de salud, requiere del acceso a determinados datos que pueden tener relevancia patrimonial[2107]. La mayoría de las veces, estas contingencias justifican situaciones de bajas o incapacidad que son solicitadas por las propias personas titulares de los datos. En este caso son también las propias leyes las que justifican este acceso[2108].

[2106] Artículo 5.1 Orden 205/2005, 8 de febrero, por la que se crea el Registro Poblacional de Cáncer de Castilla y León, que desarrolla la Ley 1/1993, 6 de abril, de Ordenación del Sistema Sanitario de Castilla.

[2107] APDCM, *Protección de datos...,* cit., 2008, p. 250.

[2108] Artículo 36 RDL 1/1994, de 20 de junio de 1994, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social: *"Deber de información por entidades financieras, funcionarios públicos y profesionales oficiales. (...)*

4. Los funcionarios públicos, incluidos los profesionales oficiales, están obligados a colaborar con la Administración de la Seguridad Social para suministrar toda clase de información, objeto o no de tratamiento automatizado, siempre que sea útil para la recaudación de recursos de Seguridad Social y demás conceptos de recaudación conjunta, de que aquellos dispongan, salvo que sea aplicable:

a) El secreto del contenido de la correspondencia.

b) El secreto de los datos que se hayan suministrado a la Administración Pública para una finalidad exclusivamente estadística. El secreto del protocolo notarial abarcará los instrumentos públicos a que se refieren los artículos 34 y 35 de la Ley de 28 de mayo de 1862 y los relativos a cuestiones matrimoniales, con excepción de los referentes al régimen económico de la sociedad conyugal.

5. La obligación de los profesionales de facilitar información de transcendencia recaudatoria a la Administración de la Seguridad Social no alcanzará a los datos privados no patrimoniales que conozcan por razón del ejercicio de su actividad, cuya revelación atente al honor o a la intimidad personal o familiar de las personas. Tampoco alcanzará a aquellos datos confidenciales de sus clientes de los que tenga conocimiento como consecuencia de la prestación de servicios profesionales de asesoramiento o defensa.

Los profesionales no podrán invocar el secreto profesional a efectos de impedir la comprobación de su propia cotización a la Seguridad Social.

A efectos del artículo 8, apartado 1, de la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, se considerará autoridad competente al Ministro de Trabajo y Asuntos Sociales, a los titulares de los órganos y centros directivos de la Secretaría General para la Seguridad Social y de la Dirección General de la Inspección de Trabajo y Asuntos Sociales, así como al Director General y a los Directores Provinciales de la Tesorería General de la Seguridad Social.

6. La cesión de aquellos datos de carácter personal, objeto de tratamiento automatizado, que se deba efectuar a la Administración de la Seguridad Social conforme a lo dispuesto en este artículo o, en general, en cumplimiento del deber de colaborar para la efectiva recaudación de los recursos de la Seguridad Social, no requerirá el

Lo mismo ocurre con las inspecciones que ha de realizar la Administración tributaria en el ejercicio de sus funciones. El deber de colaborar con la misma queda patente en la Ley[2109]. Es evidente que para poder llevar a cabo sus funciones esta Administración requiere en

consentimiento del afectado. En este ámbito, tampoco será de aplicación lo que, respecto a las Administraciones Públicas, establece el apartado 1 del artículo 21 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
En los casos en que la cesión de datos se efectúe por parte de la Agencia Estatal de la Administración Tributaria, éstos se instrumentarán preferentemente por medios electrónicos, informáticos o telemáticos"; DA Cuadragésima RDL 1/1994, 20 de junio de 1994, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social: "*Remisión de datos médicos necesarios para el reconocimiento de las prestaciones económicas de la Seguridad Social.*
En los procedimientos de declaración de la incapacidad permanente, a efectos de las correspondientes prestaciones económicas de la Seguridad Social, así como en lo que respecta al reconocimiento o mantenimiento del percibo de las prestaciones por incapacidad temporal, orfandad o asignaciones familiares por hijo a cargo, se entenderá otorgado el consentimiento del interesado o de su representante legal, a efectos de la remisión, por parte de las instituciones sanitarias de los informes, documentación clínica, y demás datos médicos estrictamente relacionados con las lesiones y dolencias padecidas por el interesado que resulten relevantes para la resolución del procedimiento, salvo que conste oposición expresa y por escrito de aquéllos.
Las entidades gestoras de la Seguridad Social, en el ejercicio de sus competencias de control y reconocimiento de las prestaciones, podrán solicitar la remisión de los partes médicos de incapacidad temporal expedidos por los servicios públicos de salud, las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social y las empresas colaboradoras, a efectos del tratamiento de los datos contenidos en los mismos. Asimismo, las entidades gestoras y las entidades colaboradoras de la Seguridad Social podrán facilitarse, recíprocamente, los datos relativos a las beneficiarias que resulten necesarios para el reconocimiento y control de las prestaciones por riesgo durante el embarazo y riesgo durante la lactancia natural". STS 25 de febrero de 2002, FJ 3, en la que se justifica este tipo de cesiones con el fin de controlar las circunstancias en que se producen bajas laborales.

[2109] Artículo 29 Ley 58/2003, 17 de diciembre 2003, General Tributaria: "*2. Además de las restantes que puedan legalmente establecerse, los obligados tributarios deberán cumplir las siguientes obligaciones:*
c) La obligación de presentar declaraciones, autoliquidaciones y comunicaciones.
d) La obligación de llevar y conservar libros de contabilidad y registros, así como los programas, ficheros y archivos informáticos que les sirvan de soporte y los sistemas de codificación utilizados que permitan la interpretación de los datos cuando la obligación se cumpla con utilización de sistemas informáticos. Se deberá facilitar la conversión de dichos datos a formato legible cuando la lectura o interpretación de los mismos no fuera posible por estar encriptados o codificados.
En todo caso, los obligados tributarios que deban presentar autoliquidaciones o declaraciones por medios telemáticos deberán conservar copia de los programas, ficheros y archivos generados que contengan los datos originarios de los que deriven los estados contables y las autoliquidaciones o declaraciones presentadas.(…)
f) La obligación de aportar a la Administración tributaria libros, registros, documentos o información que el obligado tributario deba conservar en relación con el cumplimiento de las obligaciones tributarias propias o de terceros, así como cualquier dato, informe, antecedente y justificante con trascendencia tributaria, a requerimiento de la Administración o en declaraciones periódicas. Cuando la información exigida se conserve en soporte informático deberá suministrarse en dicho soporte cuando así fuese requerido.
g) La obligación de facilitar la práctica de inspecciones y comprobaciones administrativas"; Artículo 95: "*1. Los datos, informes o antecedentes obtenidos por la Administración tributaria en el desempeño de sus funciones tienen carácter reservado y sólo podrán ser utilizados para la efectiva aplicación de los tributos o recursos cuya gestión tenga encomendada y para la imposición de las sanciones que procedan, sin que puedan ser cedidos o comunicados a terceros, salvo que la cesión tenga por objeto: a) La colaboración con los órganos jurisdiccionales y el Ministerio Fiscal en la investigación o persecución de delitos que no sean perseguibles únicamente a instancia de persona agraviada; b) La colaboración con otras Administraciones tributarias a efectos del cumplimiento de obligaciones fiscales en el ámbito de sus competencias; c) La colaboración con la Inspección de Trabajo y Seguridad Social y con las entidades gestoras y servicios comunes de la Seguridad Social en la lucha contra el fraude en la cotización y recaudación de las cuotas del sistema de Seguridad Social, así como en la obtención y disfrute de prestaciones a cargo de dicho sistema; d) La colaboración con las Administraciones públicas para la lucha contra el delito fiscal y contra el fraude en la obtención o percepción de ayudas o subvenciones a cargo de fondos públicos o de la Unión Europea. e) La colaboración con las comisiones parlamentarias de investigación en el marco legalmente establecido. (…)*". ORTIZ LIÑÁN, *Derechos y Garantías…,* cit., 2003, p. 50: "Es evidente que para suministrar información a la Administración tributaria no se requiere consentimiento del afectado"; DELGADO GARCÍA y OLIVER CUELLO, *Administración Electrónica Tributaria…,* cit., 2009, p. 37.

determinados casos, cuando la inspección se dirige a controlar las actividades económicas de determinados sujetos, caso, por ejemplo, de profesionales sanitarios, del acceso a información contenida en ficheros de los centros sanitarios. Las previsiones legales hacen que estos accesos puedan llevarse a cabo sin el consentimiento del titular de los datos[2110]. Las agencias de protección de datos han parecido defender un criterio distinto en algún caso, exigiendo la autorización de unos pacientes para que la Administración tributaria acceda a sus historias clínicas con el objetivo de inspeccionar la labor de unos profesionales sanitarios. Esta postura se ha basado en la letra de la LBAP, que no recoge expresamente la posibilidad de ceder datos a dicha administración[2111]. Sin embargo, la interpretación parece olvidar que la Ley General Tributaria reconoce explícitamente la facultad de la Administración tributaria de acceder a cualquier información para el ejercicio de sus funciones sin necesidad de recabar la autorización de su titular y que el artículo 7.3 LOPD exceptúa la exigencia de dicho consentimiento cuando así lo prevea una Ley.

Los tribunales han analizado el supuesto en que la Administración tributaria requiere a un centro sanitario el nombre de unos pacientes con fines estrictamente económicos. Se trata de controlar la actividad de ciertos profesionales sanitarios que han tratado a esos pacientes[2112]. En este caso, la identificación de estos últimos suponía relacionar a dichas personas con un tratamiento concreto por lo que esa información adquiriría relevancia sanitaria. Entienden los tribunales, que al no solicitarse toda la HC sino sólo la identificación del paciente y al tener la finalidad concreta de verificar si determinados médicos han cumplido con la obligación impuesta por la CE de contribuir al sostenimiento de los gastos públicos[2113], la cesión de dicha información es completamente acorde con el ordenamiento jurídico. Según el TS, en aplicación del principio de finalidad se deben ceder datos del centro a otra Administración con la finalidad de control tributario, pero sólo en la medida en que se trata de datos de interés económico[2114].

La decisión de los tribunales es criticable. ¿Es proporcional ceder estos datos a la Administración tributaria con el fin de que ésta controle los ingresos de determinados doctores? Se entiende aquí que el principio de proporcionalidad, concretado en los principios de pertinencia, veracidad y finalidad ya vistos, se rompe en este caso en el que se trata se identificar una serie de pacientes que fueron objeto de un tratamiento determinado. Hay que preguntarse si era necesaria la identificación de dichos sujetos. Se entiende que bastaba, para el control de los ingresos de los profesionales sanitarios, la cesión por parte del centro del número de pacientes intervenidos por los doctores, sin necesidad de identificarlos.

Con lo antedicho no se quiere concluir, ni mucho menos, que la cesión de datos sanitarios a la Administración, con la finalidad de que ésta controle los ingresos de los profesionales sanitarios o las circunstancias en que se dan las bajas u otras incapacidades a los trabajadores sea, en todo caso, contraria a derecho, pues, entre otras cosas, esta finalidad es de indudable

[2110] GONZÁLEZ MÉNDEZ, *La Protección de Datos…,* cit., 2003, p. 64.
[2111] Informe jurídico AEPD, 0242/2010.
[2112] STSJ de Asturias de 5 de junio del 2000 y STSJ de Castilla la Mancha, de 2 de junio del 2003, en el mismo sentido.
[2113] Artículo 31 CE.
[2114] STS 2 de julio de 1991.

interés público. Simplemente se quiere subrayar que en cada caso habrá que analizar qué datos son necesarios que sean cedidos, de tal manera que el daño que se vaya a realizar al derecho a la autodeterminación informativa sea el menor posible[2115].

Uno de los problemas que plantea la excepción que se estudia, no sólo en el ámbito sanitario sino en general, es que muchas veces las leyes llevan a cabo previsiones demasiado genéricas que no ayudan a favorecer la seguridad jurídica. En ocasiones las cesiones de datos se reconocen para supuestos ambiguos que pueden abrir las puertas a que se den comunicaciones de manera indiscriminada. Siguiendo la jurisprudencia del TEDH es necesario que las normas que prevean los límites al derecho que se comenta tengan cierto grado de concreción. En el sector sanitario "facilitar la asistencia médica y farmacéutica al paciente"[2116] o "el fin de que los ciudadanos reciban la mejor atención sanitaria posible"[2117] no constituyen esferas de realidad suficientemente delimitados. Una interpretación amplia de estas expresiones puede dar lugar a que se justifiquen cesiones de datos con fines que indirectamente pueden tener que ver con esos ámbitos, pero que plantean dudas sobre si se dirigen a salvaguardar la salud de las personas o no. En ocasiones suelen ser los reglamentos que desarrollan estas leyes los que concretan estas expresiones ambiguas y determinan los casos en que se deberán llevar a cabo las cesiones de datos[2118]. Ya se ha comentado más arriba el problema de legitimidad que plantea el hecho de

[2115] STJUE 20 de mayo de 2003, Rechnungshof v. Österreichischer Rundfunk y otros, asuntos acumulados C-465/00, C-138/01 y C-139/01, apunta que lo fundamental a la hora de determinar qué datos de carácter personal se pueden ceder en un determinado supuesto, es realizar un juicio de proporcionalidad. Si bien un interés general puede justificar una cesión de datos a la administración, esto no faculta al aparato público a llevar cabo cualquier operación que le venga en gana, sino sólo las que sean estrictamente necesarias para que ese interés general se vea satisfecho.

[2116] Artículo 77.8 Ley 29/2006, 26 de julio, de Garantías y Uso racional de Medicamentos y Productos Sanitarios.

[2117] Artículo 56 Ley 16/2003, de 28 mayo, de Cohesión y Calidad del Sistema Nacional de Salud.

[2118] Artículo 3 RD 1344/2007, de 11 de octubre, por el que se regula la Farmacovigilancia: "*Fuentes de información en farmacovigilancia.*

1. La información sobre los riesgos asociados a la utilización de los medicamentos puede proceder de las siguientes fuentes:

a)Notificación espontánea de casos individuales de sospechas de reacciones adversas por parte de profesionales sanitarios.

b)Estudios posautorización.

c)Bases de datos sanitarias informatizadas.

d)Información preclínica de experimentación animal.

e)Información de los ensayos clínicos de un medicamento.

f)Informaciones relacionadas con la fabricación, conservación, venta, distribución, dispensación, prescripción y utilización de los medicamentos.

g)Publicaciones científicas.

h)Otras fuentes de información, como las relativas al uso incorrecto y abuso de los medicamentos, o las correspondientes a errores de medicación, que puedan aportar datos relevantes para la evaluación de los beneficios y riesgos de los medicamentos.

i)Otras autoridades sanitarias y organismos sanitarios internacionales.

2. La Agencia Española de Medicamentos y Productos Sanitarios establecerá los convenios necesarios con los organismos competentes de las comunidades autónomas para el uso compartido de las fuentes de información que de ellas dependa señaladas en los párrafos c, f y h del apartado anterior.

3. Para facilitar el intercambio de la información sobre casos individuales de sospechas de reacciones adversas, se aplicarán las directrices elaboradas y publicadas por la Comisión Europea en el Volumen 9A de las Normas sobre medicamentos en la Unión Europea, relativas a la recopilación, verificación y presentación de notificaciones de reacciones adversas, incluyendo los requisitos técnicos en materia de intercambio electrónico de información sobre farmacovigilancia, con arreglo a los formatos acordados internacionalmente y sobre la terminología médica internacionalmente aceptada".

que sea la Administración y no el Parlamento quien determine los límites a los derechos fundamentales.

Un supuesto claro que refleja esta problemática vinculada a la relación internormativa se puede observar en la regulación de las exportaciones e importaciones de las muestras biológicas. En defensa de la salud pública es posible que sean necesarias las transmisiones de estas sustancias, incluso a nivel internacional. Piénsese en casos de epidemias que tienen efecto más allá de las fronteras del Estado. Muchas veces, a esas muestras irán vinculadas informaciones sanitarias concernientes a personas determinadas. Evidentemente estas operaciones constituirán cesiones de datos sanitarios. La regulación de las exportaciones e importaciones de este tipo de muestras se realiza fundamentalmente vía reglamentaria, si bien basándose en la propia LOPD y la normativa sanitaria[2119]. Dispone el Real Decreto por el que se establecen los requisitos para la importación y exportación de muestras biológicas, que las transmisiones que puedan darse entre diferentes instituciones, incluso dentro de la UE, no requerirán de un nuevo consentimiento del titular de los datos siempre que haya un motivo que lo justifique, fundamentalmente la protección de la salud pública[2120]. Al margen de ser discutible el que sea un reglamento el que entre a determinar esta cuestión, la regulación es un tanto confusa, sobre todo en lo que respecta al derecho a ser informado sobre los parámetros que puedan rodear a las transmisiones de los datos. Ya se ha dicho que la propia norma encomienda su justificación a una serie de leyes, la LOPD entre ellas, que pretenden dar suficiente cobertura legal como para otorgar validez al reglamento. No obstante, teniendo en cuenta que las citadas leyes no establecen una regulación concreta sobre esta materia, parece que la regulación de este contenido mediante reglamento afectaría al derecho fundamental con lo que podría dudarse de su legalidad.

I.5.2. La cesión entre administraciones.

I.5.2.A. Aspectos generales. Sobre la aplicabilidad de la excepción en el ámbito sanitario.

La cesión de datos entre diferentes administraciones se ha potenciado en los últimos años. En el ámbito interno la aprobación de la LAE ha configurado el marco adecuado para crear un flujo de información entre las administraciones y los distintos órganos de éstas[2121]. Estas comunicaciones cuentan con una regulación propia en la LOPD. En primer lugar, señala la Ley que no es necesario el consentimiento del titular cuando la transmisión se dé entre administraciones públicas y tenga por objeto el tratamiento de la información con fines históricos,

[2119] Exposición de Motivos RD 65/2006, 30 de enero de 2006, por el que se establecen Requisitos para la Importación y Exportación de Muestras Biológicas.

[2120] Artículo 10.2 RD 65/2006, 30 de enero de 2006, por el que se establecen Requisitos para la Importación y Exportación de Muestras Biológicas: "*Este Registro no será público y sólo se expedirá certificación de los datos personales inscritos en él a solicitud de la persona inscrita; de las administraciones competentes en materia de sanidad exterior o de seguridad de la Unión Europea; de terceros países o de los organismos internacionales, previa justificación por los mismos de la necesidad de los datos. A estos efectos, se entenderá prestado el consentimiento por el interesado mediante su solicitud de inclusión en el Registro, extremo del que se le informará expresamente. Cuando se expidan certificaciones para las administraciones aludidas, se les hará la advertencia de que los datos certificados no son públicos y que sólo pueden ser utilizados para la finalidad exclusiva que haya justificado la expedición de la certificación (...)*".

[2121] CERRILLO I MARTÍNEZ, "Comunicación de datos…", cit., 2010, p. 1.329.

estadísticos o científicos[2122]. En segundo lugar la Ley recoge en un apartado específico la regulación de la cesión de datos entre administraciones públicas. Dispone el artículo 21 de la norma que no podrán comunicarse datos de carácter personal entre las administraciones públicas para el ejercicio de "*competencias diferentes o de competencias que versen sobre materias distintas*". Para estos casos será necesario el consentimiento del titular, no así en los demás supuestos. Tampoco será necesaria dicha autorización cuando la transmisión entre administraciones se dé con fines históricos, estadísticos o científicos. Así ocurrirá también cuando una Administración obtenga o elabore información para otra y la comunicación de datos se produzca en este marco[2123].

De inicio no parece que esta regulación plantee mayores problemas interpretativos. Podría decirse que guarda plena coherencia con la regulación general del consentimiento, que ya se ha analizado en el capítulo anterior. Se entendía entonces que no se requiere autorización del titular para el tratamiento general de datos por las administraciones en el ejercicio de sus funciones propias[2124]. La regulación de la cesión entre administraciones vendría a dar continuación a este régimen jurídico específico. No obstante, se verá seguidamente que las dudas interpretativas que plantea la disposición que se analiza son de relevancia, cuando se trata de aplicar en la práctica[2125].

Antes de nada, teniendo en cuenta el carácter general de la excepción, cabe preguntarse, como se ha hecho antes, si esta regulación es argumentable en las cesiones de datos sanitarios. El precepto que se estudia dispone un régimen jurídico general, aplicable a todo tipo de datos. El hecho de que los que en este trabajo se comentan sean datos especialmente protegidos lleva a que se plantee la duda de si es posible la aplicación de un límite de carácter genérico a este tipo

[2122] Artículo 11.2.e) LOPD.

[2123] Artículo 21 LOPD: *"Comunicación de datos entre Administraciones públicas.-*
1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.
3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.
4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley". STC de 30 de noviembre del 2000, FFJJ 11-14, declara inconstitucional el apartado subrayado: "El motivo de inconstitucionalidad del artículo 21.1 resulta, pues, claro. La LOPD en este punto no ha fijado por sí misma, como le impone la Constitución (art. 53.1 CE), los límites al derecho a consentir la cesión de datos personales entre Administraciones Publicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 LOPD, en relación con lo dispuesto en los arts. 4, 6 y 34.e LOPD), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar. Norma que bien puede ser reglamentaria, ya que con arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso para el caso de que la modificación lo sea por una norma de similar rango, a la que crea el fichero (y ésta basta con que sea una disposición general, que no una Ley, publicada en un Boletín o Diario oficial –art. 20.1 LOPD) la que pueda autorizar esa cesión inconsentida de datos personales, lo que resulta ser, desde luego, contrario a la constitución".

[2124] Artículo 6.2 LOPD.

[2125] GUICHOT, *Datos Personales…,* cit., 2005, p. 248.

de información sensible[2126]. Para dar respuesta a esta cuestión hay que recordar los argumentos que se han dado más arriba. El artículo 8 de la LOPD señala que la regulación de los datos sanitarios se realizará de acuerdo con la normativa sanitaria, matizando que la cesión de este tipo de información deberá llevarse a cabo atendiendo a lo dispuesto en el artículo 11 de la LOPD. Nada se dice sobre la aplicación a este tipo de datos del artículo 21 que ahora se analiza. Podría pensarse, por lo tanto, que este precepto no es aplicable en este ámbito. Esta idea se podría reforzar por el hecho de que en la regulación que la Ley realiza en el artículo 7.3 del consentimiento para el tratamiento general de los datos de salud no se hace referencia a esta excepción.

La Ley no da ninguna aclaración al respecto. La Directiva europea ni siquiera cita esta excepción de manera expresa. La Recomendación del Consejo de Europa sobre protección de datos médicos no la reconoce para este ámbito. Tampoco el nuevo reglamento de desarrollo de la LOPD profundiza en esta cuestión. No obstante, al referirse a la cesión de datos sanitarios subraya que los datos de salud podrán comunicarse sin el consentimiento del titular cuando la cesión se produzca entre organismos, centros y servicios del Sistema Nacional de Salud con el fin de llevar a cabo la asistencia sanitaria.[2127]. Las agencias de protección de datos no se han detenido a analizar con profundidad el contenido de esta excepción aplicada a los datos sanitarios, sin embargo, en algún caso han aplicado el artículo 21 LOPD a la comunicación de estos datos[2128]. La jurisprudencia no ha resuelto el problema interpretativo que se analiza, siendo pocas las referencias a este artículo[2129]. Por su parte, la doctrina parece haber aceptado sin ambages la posibilidad de emplear esta excepción en las cesiones de los datos sanitarios[2130]. La aplicabilidad de este precepto a la cesión de datos sanitarios será, en todo caso, interpretable. Lo cierto es que, a pesar de que puedan encontrarse argumentos en contra, partiendo de una adecuada interpretación no hay motivo para excluir el empleo de esta disposición del ámbito sanitario.

Si bien el artículo 8 de la Ley sólo se remite al artículo 11 a la hora de determinar qué preceptos de la LOPD se aplicarán a la cesión de datos sanitarios, carece de sentido el que se atienda a dicha disposición y no al artículo 21 que ahora se analiza. Ya se criticó en su momento la redacción del artículo 8, pues podía interpretarse que con la referencia exclusiva al artículo 11 dejaba fuera del ámbito sanitario la aplicación de los demás preceptos de la Ley, entre ellos el artículo 21 y principios tan importantes como los referentes a la calidad de los datos. No parece correcto dejar de aplicar la disposición que en este momento se analiza en relación a la comunicación de los datos sanitarios.

[2126] Artículo 67.2 Ley 17/2010, 8 de noviembre, de Derechos y Deberes de las Personas en Materia de Salud en la Comunidad Foral de Navarra, cuando regula el acceso a las historias clínicas se refiere a los artículos 11.2 y 22 LOPD, sin hacer referencia al artículo 21 de la Ley, lo que podría llevar a interpretar que esta disposición no se aplica en este ámbito. TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 546-547.

[2127] Artículo 10.5 RDLOPD.

[2128] Dictamen APDCat. CNS 11/2007.

[2129] STS 15 de abril de 2002, FJ 6. Además, las pocas referencias responden, la mayoría de veces a problemas que no tienen que ver con el contenido del precepto.

[2130] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, p. 49; BACARAIA MARTRUS, "La aplicación...", cit., 2006, p. 173.

Como se ha visto, el artículo 11 se refiere al régimen general de la cesión. Por su parte, el artículo 21 de la Ley regula la misma figura pero referida concretamente a las cesiones entre administraciones. Si la cesión de los datos sanitarios ha de regularse de acuerdo a lo que dicta la LOPD, no tiene sentido que sólo se tenga en cuenta el artículo 11 y no los demás preceptos que regulan esta cuestión en la misma norma. En principio, se tendrán que tomar en consideración todas las disposiciones que entran a regular la cesión de datos. Refrenda este punto de vista el hecho de que la propia normativa sanitaria, a la que se refiere el artículo 8, vuelve a realizar una remisión genérica a la LOPD a la hora de determinar qué sujetos pueden tener acceso y de qué forma a las historias clínicas[2131]. La remisión en este caso es a toda la LOPD y no a un precepto determinado. Teniendo en cuenta que estos accesos serán en muchos casos cesiones de datos y que la referencia a la LOPD es genérica, es fácilmente interpretable que la excepción que se analiza puede tener aplicación también en las cesiones de datos sanitarios[2132].

Desde un punto de vista más sustantivo, el hecho de que los datos sanitarios sean considerados en la Ley como especialmente protegidos no puede llevar automáticamente a la inaplicación del precepto estudiado. Al igual que se hizo al analizar la remisión al artículo 11, basta con realizar una interpretación adecuada de la excepción. Esta interpretación deberá llegar, como se concluyera más arriba, de la puesta en común de la normativa de protección de datos y de la sanitaria.

Teniendo en cuenta que el ordenamiento no aclara el alcance que puede tener la excepción en el ámbito sanitario, no es tarea fácil determinar de qué manera pueden transmitirse los datos entre las distintas administraciones en este campo. Si bien es perfectamente aceptable la aplicabilidad de la excepción en el ámbito sanitario, no parece que pueda asumirse como norma general, y sin establecer límite alguno, la posibilidad de que en todo caso se comuniquen datos sanitarios de un paciente a una Administración, sea cual sea, para que esta última pueda llevar a cabo sus funciones, cualquiera que éstas sean. Hay que volver a recordar que en última instancia se está hablando de proteger la intimidad y el derecho a la autodeterminación informativa de las personas. No parece correcto admitir prima facie la posibilidad de que se establezca un flujo ilimitado de información sanitaria, cualquiera que sea su contenido, entre las diferentes administraciones.

Necesariamente deberá ser el principio de finalidad el que establezca los límites entre los que deberá situarse este flujo de datos sanitarios. La propia Ley da pie, como se verá, a que se pueda llevar a cabo una interpretación coherente con este principio.

I.5.2.B. El principio de finalidad como criterio delimitador del ámbito de aplicación de la excepción.

El artículo 21.1 de la Ley señala que no se podrán comunicar datos de carácter personal entre administraciones, sin el consentimiento o habilitación legal pertinente, para el ejercicio de "competencias diferentes o de competencias que versen sobre materias distintas". El uso que se

[2131] Artículo 16.3 LBAP.
[2132] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 85.

da en la norma a los conceptos "competencia" y "materia" ha dado lugar a equívocos[2133]. El empleo de la conjunción disyuntiva "o" tampoco ayuda a aclarar el contenido de este precepto[2134]. Lo cierto es que de la lectura de la disposición no queda claro cuál es el ámbito de aplicación de la excepción[2135]. Caben por lo tanto diferentes interpretaciones al respecto.

Cuando se hace referencia al concepto de materia hay que relacionar dicho término con el de finalidad. Una acción afectará a una materia o a otra dependiendo de la finalidad que persiga. En el caso que aquí interesa, por ejemplo, las acciones que afectan a la materia sanitaria se identificarán porque persiguen, de una manera más o menos inmediata, la finalidad de proteger la salud de las personas. El concepto de competencia, por su parte, se ha de identificar con el de potestad, entendida como facultad que se tiene sobre determinados aspectos de una materia. Partiendo de estas aclaraciones pueden distinguirse diferentes interpretaciones del precepto de la LOPD que se comenta.

En principio, si se interpretara la disposición en sentido literal, una Administración podría ceder datos de carácter personal a otra sin recabar el consentimiento del titular, sólo cuando esta última fuera a ejercer las mismas competencias sobre la misma materia que la Administración cedente[2136]. Si, según la Ley, no se puede comunicar información de carácter personal a otra Administración para desarrollar competencias o materias diferentes, parece que la única opción es que la cesión se dé para llevar a cabo la misma competencia sobre la misma materia. Puede llegar a desprenderse de la letra de la Ley que esta cesión sólo estará justificada cuando se produzca entre órganos que tengan las mismas atribuciones o funciones[2137]. En algún momento ha parecido reconocerse, si bien después de criticar la letra de la Ley basándose fundamentalmente en argumentos de Derecho comparado, que ésta es la interpretación admitida en el ordenamiento interno, aplicable también en el ámbito sanitario[2138].

Esta interpretación reduciría la aplicabilidad de esta excepción a supuestos muy concretos. Se ha entendido que este criterio constituiría un límite al privilegio que tienen las administraciones en el tratamiento de datos[2139]. Como se ha ido viendo a lo largo de este trabajo, son numerosas las excepciones recogidas en la Ley a las facultades de los titulares de datos para favorecer la capacidad de la Administración de manipular información en el ejercicio de sus funciones. El aparato público cuenta con ciertas facilidades para tratar los datos de la ciudadanía. Pues bien, una interpretación restrictiva del precepto vendría a limitar este privilegio.

[2133] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 236; GUICHOT, *Datos personales…,* cit., 2005, p. 251; CERRILLO I MARTÍNEZ, "Comunicación de datos…", cit., 2010, p. 1.314.

[2134] BACARIA MARTRUS, "La Aplicación…", cit., 2006, p. 173.

[2135] Dictamen AVPD CN09-009, 7 de abril de 2009, se pone de manifiesto la dificultad de comprender el alcance de esta excepción, en el caso concreto en que un Ayuntamiento solicita cierta información a una Diputación Foral.

[2136] Informes jurídicos complementarios a la exposición realizada por el Consejero de Sanidad del Gobierno Vasco durante su comparecencia ante la Comisión de Sanidad del Parlamento Vasco el 23 de mayo de 2002, a fin de dar cuenta del proceso de centralización de los datos de los pacientes recogidos en los centros de salud de Osakidetza. MURILLO DE LA CUEVA, *Informática y...*, cit., 1993, p. 97; VALERO TORRIJOS, *Comentarios a la Ley…*, cit., 2001, p. 238.

[2137] GAY FUENTES, *Intimidad y Tratamiento…,* cit., 1995, p. 97

[2138] TRONCOSO REIGADA, *e-PRODAT: Administración…,* cit., 2006, pp. 24-25; TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 85.

[2139] FERNÁNDEZ GARCÍA, "Comunicación de datos entre…", cit., 2008, pp. 425-428

De asumirse esta interpretación la excepción sólo podría aplicarse a las relaciones inter-administrativas, en las que se encuentran diferentes administraciones que cuentan con la misma competencia sobre la misma materia. Se admitiría por ejemplo la cesión de datos entre órganos de diferentes administraciones con competencias en el ámbito sanitario dirigidas a ejercer la potestad sancionadora. En cambio, no podría admitirse la comunicación entre administraciones, sin consentimiento del titular de los datos, que, aun ejerciendo funciones sobre la materia sanitaria, tuvieran competencias diferentes.

Es posible entender el precepto que ahora se analiza de otra manera[2140]. En contraposición al criterio expuesto se puede realizar una interpretación especialmente amplia de la excepción. Partiendo de los principios de cooperación y coordinación que según las leyes han de guiar las relaciones entre las diferentes administraciones, puede llegar a justificarse la transmisión, incluso indiscriminada, de información entre los entes públicos[2141]. Este flujo ilimitado de datos entre las administraciones podría encontrar apoyo en la LOPD. Como se vio en el capítulo anterior, la Ley permite el tratamiento de datos por las administraciones sin el consentimiento del titular cuando éstos sean empleados "*para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias*"[2142]. Cualquier Administración puede tratar información sobre un ciudadano determinado sin su consentimiento para el ejercicio de las funciones que se corresponden con sus competencias. La cesión no es más que una vía para habilitar un nuevo tratamiento. Si la Administración cesionaria recaba la información para emplearla en el ejercicio de sus funciones podría plantearse aplicar la citada previsión, que permitiría recoger los datos sin necesidad de solicitar el consentimiento del titular. Así, se podría concluir que debería ser válida cualquier cesión entre administraciones diferentes, independientemente de que las competencias y las materias sobre las que ejerce sus funciones la Administración cesionaria sean diferentes a las ejercidas por la Administración cedente. Bastaría con que el órgano cesionario manipulara la información en el ejercicio de sus funciones. Tendría sentido esta interpretación por cuanto que, en todo caso, la excepción al consentimiento vendría justificada por la defensa del interés general. Se refuerza este punto de vista atendiendo al hecho de que todo tratamiento ha de respetar unos principios de calidad mínimos, lo que garantiza que cada Administración manipulará los datos oportunos únicamente para llevar a cabo las funciones que le corresponden por Ley[2143]. Necesariamente, si estos principios se cumplen, no hay motivo para que los ciudadanos puedan pensar que sus datos son tratados por la Administración de manera irregular, con fines desconocidos.

La excepción que ahora se analiza se puede comprender, por lo tanto, desde una perspectiva tanto restrictiva como amplia. Concluir cómo ha de entenderse este contenido no es tarea fácil.

[2140] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 243, que basa su argumentación en la creación de proyectos como la Ventanilla Única.

[2141] Artículo 4 LPAC: "*Principios de relaciones entre las Administraciones públicas. 1. Las Administraciones públicas actúan y se relacionan de acuerdo con el principio de lealtad institucional y, en consecuencia, deberán: (…)*
c) Facilitar a las otras Administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias
d)Prestar, en el ámbito propio, la cooperación y asistencia activas que las otras Administraciones pudieran recabar para el ejercicio de sus propias competencias."

[2142] Artículo 6 LOPD.

[2143] GUICHOT, *Datos Personales…,* cit., 2005, pp. 256-257.

Una interpretación restrictiva podría llevar a entorpecer la labor de los profesionales sanitarios. Pero, por otro lado, una visión excesivamente amplia podría llevar a crear un marco en el que la Administración pudiera manipular los datos de las personas de manera indiscriminada e incontrolada.

La interpretación estricta del artículo que se comenta tiene la dificultad de tener que delimitar con precisión las competencias que corresponden a cada Administración sobre cada materia. Una vez delimitadas, las cesiones sin consentimiento del titular sólo podrán realizarse entre los sujetos que llevan a cabo dichas competencias. Los datos no podrán transmitirse sin el consentimiento del afectado o sin habilitación legal más allá del ámbito marcado, independientemente de que se trate de una comunicación a un órgano que ejerce su actividad dentro de la misma materia, en este caso sanitaria. La asunción de esta interpretación reduciría en exceso la aplicabilidad de la excepción[2144], pudiendo incluso suponer un obstáculo en la eficiente realización de la labor de los profesionales sanitarios. Hay que tomar en consideración que a falta de una norma que concrete la aplicación de este límite en el ámbito que se trata, la indeterminación de los conceptos que se emplean en la Ley puede crear en la práctica una innecesaria inseguridad entre los profesionales sanitarios. Los diferentes órganos que componen las distintas administraciones que cuentan con competencias en materia sanitaria y que ejercen funciones diferentes (investigadoras, de asistencia, de inspección, etc.), podrían encontrarse ante la duda de si es posible aplicar la excepción a las cesiones de datos que puedan realizar entre sí.

Por su parte, la interpretación más amplia conllevaría la posibilidad de que exista un flujo ilimitado de información entre las diferentes administraciones. Este punto de vista ha sido criticado[2145]. Cierto es que en términos generales esta interpretación redundaría en beneficio de un funcionamiento más ágil de la Administración que, incluso a falta de habilitación legal, no tendría que solicitar autorización alguna del titular de los datos para trasladar la información a otra Administración, con independencia de la materia sobre la que ejerza sus competencias. Sin embargo, esta posibilidad ha de ser rechazada cuando se trata de datos sanitarios.

El que pueda quedar en manos, exclusivamente, de órganos administrativos la decisión de ceder o no los datos sanitarios a otras administraciones ha de ser vista de inicio con temor o precaución. En primer lugar porque no hay que olvidar que los riesgos que plantea la cesión son mayores a los que plantea cualquier otra operación de tratamiento. Evidentemente, esta interpretación facilita el flujo de información. Y cuanto mayor es este flujo mayor es el riesgo de que los datos puedan ser empleados de manera torticera. Las nefastas consecuencias que puede acarrear un uso no deseado de la información sanitaria ya se han puesto de manifiesto. En segundo lugar, porque las facultades de control por parte del titular de los datos se verían reducidas sobremanera con la aplicación de la interpretación tan amplia de la excepción. Sería la propia Administración la que decidiría cuándo y cómo ceder los datos, aunque es cierto que estas cesiones deberían guardar, en todo caso, una serie de garantías. Por un lado, atendiendo al

[2144] GAY FUENTES, *Intimidad y Tratamiento…,* cit., 1995, p. 97: "que los órganos administrativos entre los cuales vayan cruzarse datos deben tener el mismo tipo de atribuciones –normativas o ejecutivas y dentro de éstas, del mismo tipo, de inspección, de sanción, de gestión, etc.- sobre idénticas materias. Realmente los supuestos de este tipo son escasos, en la medida en que el sistema de distribución de competencias tiende en su conjunto a evitarlos".
[2145] DEL PESO NAVARRO, *Ley de Protección…,* cit., 2000, p. 63.

principio de finalidad, la Administración cesionaria sólo podría emplear los datos para llevar a cabo las funciones que por Ley le corresponden. Por otro, según reconoce la LOPD, las disposiciones que crean los ficheros de las administraciones, que contienen los datos que se pretenden comunicar, deberían prever las cesiones de datos que se quieran llevar a cabo. Así, en teoría, las cesiones entre administraciones no se podrían llevar a cabo con absoluta arbitrariedad. No obstante, la práctica ha enseñado que la ambigüedad empleada tanto a la hora de definir las funciones de los órganos administrativos, como a la hora de determinar las cesiones que se pretenden, exige tomar ciertas cautelas, cuando menos si se trata de datos que son reconocidos por la Ley como especialmente protegidos. Son conocidos distintos supuestos en que las cesiones de datos sanitarios entre clínicas privadas y administraciones, con fines que nada tienen que ver con la protección de la salud, como puede ser llevar a cabo un estudio lingüístico, han causado cierta alarma[2146].

La propia jurisprudencia ya alertó sobre el peligro de dejar en manos de la Administración la facultad de decidir cuándo se pueden llevar a cabo las cesiones de datos sin el consentimiento del titular. Entendió que esta facultad podría encubrir una capacidad de la Administración de establecer límites al derecho a consentir. La fijación de los límites de los derechos fundamentales, como no puede ser de otra forma, corresponde al Legislador y no a la Administración. Este argumento se empleó para declarar la inconstitucionalidad de diferentes aspectos de la LOPD[2147]. Si los tribunales señalan la inconveniencia de que la Administración pueda determinar, a través de normas de rango infralegal, cuándo pueden ceder datos a otras administraciones, parece que la aceptación de una habilitación general o absoluta que permita en cualquier caso la transmisión de cualquier dato a otra Administración, incluso para llevar a cabo finalidades que nada tienen que ver con la que motivó la recogida de datos originariamente, tiene difícil encaje en la Ley, por lo menos si se está hablando de datos que la propia norma entiende que son inicialmente merecedores de especial protección. En esta línea los tribunales han negado en casos concretos la posibilidad de que una Administración acceda a datos de salud de una persona, sin su consentimiento o amparo legal suficiente, para el cumplimiento de fines que si bien tienen indudable interés general, nada tienen que ver con los que motivaron su recogida inicial[2148]. Más concretamente, han considerado que no es posible la comunicación de datos médicos indiscriminada entre diferentes administraciones con fines que nada tienen que ver con la protección de la salud[2149].

[2146] Diario El Mundo, 14 de diciembre de 2006. Resolución AEPD, R/00007/2007, de 10 de enero de 2007, procedimiento PS/00088/2006. SAN 27 de febrero de 2008.

[2147] STC 30 de noviembre del 2000, FFJJ 13 y 14. En los que se declara la inconstitucionalidad de un inciso del artículo 21.1 LOPD, que permite la cesión sin consentimiento entre administraciones "*cuando la comunicación hubiere sido prevista por las disposiciones de creación de fichero o por disposiciones de superior rango que regule su uso*". Entiende el TC que esta disposición facultaría a la Administración para establecer límites a un derecho fundamental a través de reglamentos, vulnerando así el principio de reserva de Ley que garantiza que sea el representante del pueblo el que determine los límites de los derechos fundamentales.

[2148] STC 23 de marzo de 2009, FFJJ 2 y 3: en la que reconoce que el acceso de la Administración a los datos de salud de una persona ha de estar justificada en una Ley, sin que baste con que la Administración acceda a dicha información para llevar a cabo sus funciones.

[2149] STC 29 de junio de 2009, FFJJ 4 y 5: en este caso los datos médicos extraídos de un proceso selectivo para acceder al cuerpo de la Ertzaintza son empleados, previa cesión de datos entre las pertinentes administraciones, para excluir a dicha persona de otro proceso selectivo en otra Administración. Se entiende que a pesar de que el uso de los datos

Atendiendo a lo que se ha dicho sobre las diferentes interpretaciones, se entiende que debería adoptarse un criterio intermedio que permitiera la cesión entre diferentes administraciones con distintas competencias, pero sobre un mismo fin. Teniendo en cuenta el carácter vertebral del principio de finalidad en materia de protección de datos[2150], y poniendo en relación el artículo 21.1 LOPD con el resto del articulado de la Ley, es posible apoyar este criterio[2151].

La clave residiría en equiparar, como se ha hecho más adelante, el concepto de materia con el de finalidad. Este punto de vista permite sustentar una posición que reconoce la posibilidad de ceder datos entre administraciones que tengan competencias o potestades diferentes pero actúan para llevar a cabo la misma finalidad, es decir, actúan sobre la misma materia. Así, en la medida en que se cumple con el principio de finalidad y la cesión se da entre administraciones que van a desarrollar sus competencias dentro de una misma materia, la excepción sigue teniendo pleno sentido[2152]. Sólo las cesiones entre diferentes administraciones para el cumplimiento de diferentes finalidades, es decir, entre administraciones que actúan sobre materias diferentes, deberán contar con la autorización del titular de los datos o estar previstas en una Ley que legitime dichas comunicaciones[2153].

Desde un punto de vista práctico, la interpretación que se sigue facilita la labor de la Administración pública, pues se amplía el ámbito de aplicación de la excepción. Podría pensarse que se limita en exceso el derecho a la autodeterminación informativa. La necesidad de crear un flujo ágil de información entre las instituciones no puede desembocar en otorgar a la Administración la facultad de limitar el derecho a la autodeterminación informativa de manera arbitraria, mucho menos cuando se trata de datos cuyo uso inadecuado puede tener consecuencias especialmente negativas. Este riesgo, sin embargo, queda salvado con la interpretación que aquí se defiende. Y es que en la medida en que el titular de los datos tiene la seguridad de que el principio de finalidad va a regir estas cesiones de datos, se garantiza que la información que le concierne se va a emplear dentro de un ámbito determinado que el propio afectado conoce.

Esta posición cobra más sentido en la actualidad, en la medida en que se está fomentando la interconexión de las bases de datos de las distintas administraciones para el funcionamiento más efectivo de las mismas[2154]. En la propia normativa sanitaria pueden encontrarse ejemplos en que basar esta posición. La apuesta por una historia clínica única es uno de ellos, pues se trata de un instrumento que requiere de la cesión de datos entre diferentes administraciones, especialmente

médicos por parte de la Administración cesionario se lleve a cabo con fines de interés público, la cesión no está legitimada. SAN 27 de febrero de 2008, FJ 2, en la que se decide sobre la pertinencia o no del acceso a datos sanitarios para el control del uso del catalán en los centros sanitarios, señalando la necesidad de adoptar todas las garantías, como la anonimización, para llevar a cabo esta labor.

[2150] STSJ de Cataluña 19 de diciembre de 2006, FJ 3. TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, pp. 984-985, subraya la relevancia de comprender el artículo 21 LOPD atendiendo al principio de finalidad.

[2151] CERRILLO I MARTÍNEZ, "Comunicación de datos…", cit., 2010, p. 1.316, también parece fundamentar la interpretación de esta excepción en el principio de finalidad; TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, p. 530.

[2152] GUICHOT, *Datos Personales…,* cit., 2005, pp. 250-251.

[2153] GUICHOT, *Datos Personales…,* cit., 2005, p. 255.

[2154] GAMERO CASADO, *Legislación de Administración…,* cit., 2008, pp. 15 y 16.

entre la Administración estatal y la autonómica[2155], y entre distintos órganos que cumplen funciones diversas dentro del ámbito sanitario[2156]. Una interpretación restrictiva de la excepción que se comenta podría tener un efecto limitativo de esta nueva posibilidad que plantea la Administración electrónica[2157].

El mejor funcionamiento de la Administración en la defensa de intereses públicos exige que se establezcan excepciones a los derechos fundamentales. La relevancia de lo antedicho se refleja en leyes que regulan materias relacionadas con el tratamiento de datos, asociados o disociados, en las que se subraya la importancia de la transmisión de la información entre diferentes administraciones. Ya se han expuesto, en el apartado relativo a la cesión de datos sin consentimiento del titular por prescripción legal, diferentes ejemplos de leyes que prevén la transmisión de información entre administraciones.

Se justifica, en definitiva, la cesión de datos entre administraciones, que a pesar de contar con competencias diferentes actúan sobre la misma materia. De esta manera, y siendo coherentes con la relevancia que se ha dado al principio de finalidad, en el ámbito estrictamente sanitario es admisible que la finalidad de salvaguardar la salud de las personas justifique las comunicaciones entre las administraciones que actúan en el sector sanitario. La aplicación de la excepción, sin embargo, no evitará que sea necesario que se respeten los demás principios de calidad, fundamentalmente el de proporcionalidad. Es decir, no se plantea que dentro de los sistemas sanitarios el flujo de información sea indiscriminado. En este sentido, habrá que atender al principio de pertinencia, a la necesidad de justificar por cada cesionario el acceso a los datos que pretende. Esta interpretación se reforzará al estudiar la excepción al derecho a consentir una cesión de datos cuando el tratamiento se dirige a la protección de la salud de las personas. Y es que, como se verá, en lo que aquí interesa, independientemente de la aplicabilidad o no de la excepción en el ámbito sanitario, el ordenamiento reconoce la posibilidad de realizar cesiones de datos sanitarios entre diferentes administraciones cuando la finalidad sea la protección de la salud de las personas.

[2155] DA Tercera LBAP: "*El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición*".

[2156] Artículo 16 LBAP: "*4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.*

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria".

[2157] PÉREZ VELASCO, "Los Ficheros...", cit., 2005, p. 2; PÉREZ VELASCO, "La Potestad…", cit., 2004.

I.5.2.C. Algunos apuntes sobre el alcance de la excepción: su aplicabilidad a las cesiones entre órganos administrativos y a las comunicaciones a los colegios profesionales.

Aceptada la cesión de datos sin consentimiento del titular entre diferentes administraciones cuando su actividad se dirige a la consecución de una misma finalidad, es necesario realizar algunos apuntes en relación al alcance de dicha excepción.

A) En primer lugar, e independientemente de la interpretación que se haga del precepto, hay que volver a recordar que el hecho de que la cesión de datos de carácter personal entre administraciones sin el consentimiento del titular de los datos esté justificada, no quita para que los demás principios que salvaguardan el derecho a la autodeterminación informativa hayan de ser tomados en cuenta, y tengan que adoptarse las medidas de seguridad correspondientes. No hay que olvidar que incluso la Administración ha llevado a cabo operaciones que atentan contra los derechos fundamentales de las personas[2158]. La necesidad de guardar unas garantías mínimas en estos casos, dirigidas a la protección de la autodeterminación informativa se recoge expresamente, más allá de la LOPD, en las normas que regulan diferentes realidades que afectan a la protección de datos[2159].

En concreto, dejando a un lado las medidas de seguridad y el respeto a los principios que determinan la calidad de los datos, resulta fundamental que también en el ámbito público el deber de informar se lleve a cavo con total rigurosidad, pues el tratamiento de los datos de los ciudadanos no puede realizarse completamente al margen de estos últimos[2160]. Teniendo en cuenta la extensión de la excepción al consentimiento aplicable a las distintas operaciones que lleva a cabo la Administración, la única posibilidad del titular de controlar lo que sucede con los datos que le conciernen es respetando rigurosamente el derecho a ser informado. Es necesario, salvo que medie causa justificante, que el titular de los datos sea informado de las cesiones que vayan a llevar a cabo las administraciones entre ellas. Cierto es que la propia Ley, cuando regula la creación, modificación y supresión de los ficheros públicos, señala que cuando se cree o modifique un fichero deberán indicarse, entre otros puntos, las cesiones de datos previstas[2161].

[2158] Son innumerables los supuestos en que las administraciones públicas han sido sancionadas por vulnerar la normativa protectora de los datos de carácter personal. Casos, por ejemplo, en que la Administración ha puesto al descubierto las matrículas de los vehículos privados de determinados jueces, Resolución AEPD, R/01722/2008, 5 de diciembre de 2008, procedimiento AP/00041/2008.

[2159] Artículo 15.1 Ley 12/1989, de 9 de mayo, de la Función Estadística Pública: *"La comunicación a efectos estadísticos entre las administraciones y organismos públicos de los datos personales protegidos por el secreto estadístico sólo será posible si se dan los siguientes requisitos, que habrán de ser comprobados por el servicio u órgano que los tenga en custodia:*
a) Que los servicios que reciban los datos desarrollen funciones fundamentalmente estadística y hayan sido reguladas como tales antes de que los datos sean cedidos.
b) Que el destino de los datos sea precisamente la elaboración de las estadísticas que dichos servicios tengan encomendados.
c) Que los servicios destinatarios de la información dispongan de los medios necesarios para preservar el secreto estadístico. En relación a este punto concreto ver TORRE SERRANO, "Administración Estadística...", cit., 1999, pp. 527-539.

[2160] GARCÍA-BERRIO HERNÁNDEZ, *Informática y Libertades...*, cit., 2003, p. 224.

[2161] Artículo 20.2 LOPD: *"las disposiciones de creación o de modificación de ficheros deberán indicar, entre otras cosas, e) las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros"*.

No obstante, más allá de esta acción, es necesaria una información más personalizada y concreta, atendiendo a los parámetros que se citaron al analizar el derecho a ser informado. Tal como ha especificado la doctrina, las nuevas tecnologías facilitan que este derecho se lleve a cabo con las máximas garantías[2162]. El uso de Internet hace posible que se pueda llegar con mayor facilidad a los ciudadanos, para que tengan conocimiento de lo que se está haciendo o se puede hacer con sus datos.

B) En segundo lugar hay que realizar otro apunte de interés. Los criterios que la Ley establece para que la cesión de datos de carácter personal sea válida no sólo hay que entenderlos aplicables a las cesiones entre diferentes administraciones, sino también a las comunicaciones entre diferentes órganos de una misma Administración, más allá de las dudas que genera la consideración de estas operaciones como cesiones[2163]. La LOPD no hace referencia expresa a este supuesto, sin embargo, no puede aceptarse que la cesión de información entre diferentes órganos de la misma entidad pueda llevarse a cabo de cualquier manera, al margen de las garantías dispuestas por la Ley[2164]. En estos casos también será de aplicación la excepción al consentimiento que se recoge en la norma para las cesiones entre distintas administraciones. Tiene sentido esta apreciación en la medida en que la mayoría de procedimientos administrativos pasan por diferentes órganos de una misma Administración. Carecería de coherencia que cada transmisión de información entre estos órganos tuviera que requerir la autorización del titular de los datos, máxime si se tiene en cuenta que la cesión entre diferentes administraciones genera, sin duda alguna, mayores riesgos para la intimidad y el derecho a la autodeterminación informativa, y a esta última operación sí le es aplicable, en muchos casos, la citada excepción[2165]. Hay que tener en cuenta que el mismo interés general que defiende una Administración lo defienden, obviamente, los distintos órganos que la componen.

C) En tercer lugar, dispone la Ley que cuando una Administración recoge datos para otra no es necesario el consentimiento del titular para que se produzca la transmisión entre ambas. En estos supuestos la Administración cedente simplemente recaba información de carácter personal para transmitírsela a otra, que será la que la manipule.

Podría pensarse que la Administración que recaba los datos no es más que una mera encargada del tratamiento[2166]. En la medida en que no lleva a cabo un tratamiento, entendido en sentido estricto, podría realizarse esta interpretación. Si así fuera, la operación realizada no sería otra cosa que un "acceso por cuenta de tercero". Por lo tanto, deberían cumplirse las condiciones

[2162] TRONCOSO REIGADA, *e-PRODAT: Administración…,* cit., 2006, p. 23.
[2163] TRONCOSO REIGADA, *La Protección de Datos…*, cit., 2010, pp. 440-441, niega que las transmisiones de datos entre unidades de una misma Administración sean cesiones.
[2164] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 237; GARCÍA-BERRIO HERNÁNDEZ, *Informática y Libertades...*, cit., 2003, pp. 227-228.
[2165] FREIXAS GUTIERREZ, *La Protección...*, cit., 2001, pp. 236-237; FERNÁNDEZ SALMERÓN, *La Protección...*, 2003, cit., pp. 234-235: "Resulta evidente que las limitaciones que impone este precepto (artículo 11 de la LOPD) a la cesión de datos personales son más estrictas que las dispuestas por el artículo 21 LOPDP, de modo tal que no tendría demasiado sentido sujetar a mayores exigencias la cesión entre órganos de una misma Administración Pública que la realizada entre Administraciones Públicas distintas"; FERNÁNDEZ GARCÍA, "Comunicación de datos entre…", cit., 2008, pp. 428 y 430.
[2166] GUICHOT, *Datos Personales…,* cit., 2005, p. 248.

que establece el artículo 12 de la Ley, fundamentalmente la formalización de un contrato en el que deberían concretarse las condiciones del tratamiento de los datos.

No parece que la operación a la que ahora se hace referencia pueda tener la consideración de acceso por cuenta de tercero. Así puede deducirse de la jurisprudencia que en algún caso ha aplicado el artículo 21 para supuestos en que no se cita contrato alguno que determine las condiciones de la cesión[2167]. La necesidad de formalizar este contrato carece de sentido. La mayoría de las veces el acceso a datos por cuenta de un tercero hace referencia a casos en que una empresa manipula datos en nombre de otra que es la responsable. En el supuesto que se analiza, por el contrario, la situación es diferente: el órgano cedente se limita a recabar información para transmitirla al que será el responsable, pero no lleva a cabo manipulación alguna más allá de la recogida de datos.

Lo dicho no quiere decir que el cedente no deba cumplir con las condiciones que marca la Ley para la recogida de datos. En todo caso deberá respetar los principios que guían la protección de datos, fundamentalmente la obligación de informar. Hay que tener en cuenta que en este supuesto la Ley no establece mayores condiciones para llevar a cabo la transmisión, sin que tan siquiera se fije la necesidad de que las diferentes administraciones o los diferentes órganos se dediquen a la misma finalidad.

D) En cuarto lugar, al igual que ocurre con los órganos de las administraciones, puede preguntarse si la excepción que se estudia es aplicable a la cesión de datos sanitarios a los Colegios Oficiales de médicos. Mucho se ha discutido sobre la naturaleza jurídica de estas instituciones[2168]. Su consideración como sujeto público o privado ha sido debatida en innumerables ocasiones, partiendo de la distinción que realiza la propia Constitución entre asociaciones de libre creación, organizaciones profesionales que contribuyen a la defensa de intereses económicos y los Colegios Profesionales[2169]. Más allá de esta cuestión, lo que aquí interesa saber es si estas instituciones llevan a cabo funciones de carácter público, que puedan justificar la aplicación de la excepción.

La normativa reguladora de los Colegios Profesionales y los estatutos de los diferentes colegios de médicos no dejan lugar a duda del carácter público de algunas actividades de estas entidades. Su calificación, en la normativa que regula esta figura, como corporaciones de derecho público deja claro que pueden identificarse en su actuación funciones de interés

[2167] SAN 24 de septiembre de 2008, FJ 3.

[2168] ARIÑO ORTIZ y SOUVIRÓN, *Constitución y Colegios…,* cit., 1984, p. 127; FANLO LORAS, *El debate sobre colegios…,* cit., 1992, p. 31; DEL SAZ, *Los Colegios Profesionales…,* cit., 1996, p. 140; LÓPEZ GONZÁLEZ, *Los Colegios Profesionales…,* cit., 2001, p. 51.

[2169] Artículo 22 CE: "*1. Se reconoce el derecho de asociación (…)*"; Artículo 36 CE: "*La Ley regulará las peculiaridades propias del régimen jurídico de los Colegios Profesionales y el ejercicio de las profesiones tituladas. La estructura interna y el funcionamiento de los Colegios deberán ser democráticos*"; Artículo 52 CE: "*La Ley regulará las organizaciones profesionales que contribuyan a la defensa de los intereses económicos que les sean propios. Su estructura interna y funcionamiento deberán ser democráticos*". SOUVIRÓN MORENILLA, *Naturaleza y Caracteres…,* cit., 1980, p. 7; ARIÑO ORTIZ y SOUVIRÓN, *Constitución y Colegios…,* cit., 1984, pp. 92-96; SÁNCHEZ SAUDINÓS, *Los Colegios Profesionales…,* cit., 1996, p. 78; DEL SAZ, *Los Colegios Profesionales…,* cit., 1996, p. 57; FANLO LORAS, "Encuadre Histórico y Constitucional…", cit., 1996, p. 79.

general[2170]. En este sentido, la jurisprudencia, si bien reconoce que estas organizaciones se crean para defender los intereses privados de los colegiados, subraya la existencia entre sus actividades de finalidades de interés público[2171]. No hace falta profundizar en exceso para darse cuenta que una adecuada ordenación de la actividad médica redundará en beneficio de toda la sociedad. La propia AEPD ha reconocido que los ficheros de estos organismos son ficheros de titularidad pública, resultándoles aplicable el artículo 21 de la LOPD[2172].

Como se puede intuir, el problema reside en identificar cuándo se está en el ejercicio de las citadas funciones de interés común. En términos generales, cuando la actividad se dirige a satisfacer las necesidades no tanto de los colegiados, sino de los destinatarios de la actividad profesional colegiada, se puede entender que se están llevando a cabo actividades de interés público[2173], que son básicamente las consideradas funciones esenciales de la institución colegial[2174]. En lo que aquí concierne, éstas son fundamentalmente la actividad organizativa, disciplinaria y de resolución de conflictos[2175]. En la medida en que los Colegios Oficiales de

[2170] Artículo 1 Ley 2/1974, 13 de febrero de 1974, sobre Colegios Profesionales: "*1. Los Colegios Profesionales son Corporaciones de derecho público, amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines*"; Artículo 1 RD 1018/1980, de 19 de mayo, por el que se aprueban los Estatutos Generales de la Organización Médica Colegial y del Consejo General de Colegios Oficiales de Médicos: "*La Organización Médica Colegial se integra por los Colegios provinciales oficiales de médicos y por el Consejo General, que son corporaciones de derecho público, amparadas por la Ley General de Colegios Profesionales, con estructuras democráticamente constituidas, carácter representativo y personalidad jurídica propia, independientes de la Administración del Estado, de la que no forman parte integrante, sin perjuicio de las relaciones de derecho público que con ella legalmente les correspondan*"; Artículo 1 Estatutos del Colegio Oficial de Médicos de Bizkaia, aprobados en 27 de enero de 1991: "*El Colegio Oficial de Médicos de Bizkaia es una Corporación de Derecho Público (...)*".

[2171] STC 18 de febrero de 1988, FJ 4; SAN 26 de febrero de 2008, FJ 3. ARIÑO ORTIZ y SOUVIRÓN, *Constitución y Colegios…,* cit., 1984, pp. 118-124; FANLO LORAS, *El debate sobre colegios…,* cit., 1992, pp. 71-72.

[2172] Informe jurídico de la AEPD, "Naturaleza de los ficheros colegiales", 2002.

[2173] SÁNCHEZ MORÓN, *Derecho Administrativo…,* cit., 2007, p. 415; Revista de la APDCM, *Datospersonales.org,* nº 26, marzo de 2007: puede ponerse como ejemplo de estas actividades de interés común la creación, a iniciativa del Colegio Oficial de Médicos de Madrid, de una base de datos con la historia clínica de los centros sanitarios privados, para facilitar la labor de los profesionales.

[2174] Artículo 5 Ley 25/2009, 22 de diciembre de 2009, de modificación de Diversas Leyes para su Adaptación a la Ley sobre el Libre Acceso a las Actividades de Servicios y su Ejercicio, que reforma el artículo 3.1 Ley 2/1974, 13 de febrero de 1974, sobre Colegios Profesionales: "*Son fines esenciales de estas Corporaciones la ordenación del ejercicio de las profesiones, la representación institucional exclusiva de las mismas cuando estén sujetas a colegiación obligatoria, la defensa de los intereses profesionales de los colegiados y la protección de los intereses de los consumidores y usuarios de los servicios de sus colegiados, todo ello sin perjuicio de la competencia de la Administración Pública por razón de la relación funcionarial*". ARIÑO ORTIZ y SOUVIRÓN, *Constitución y Colegios…,* cit., 1984, pp. 122-123; SÁNCHEZ SAUDINÓS, *Los Colegios Profesionales…,* cit., 1996, p. 267; DEL SAZ, *Los Colegios Profesionales…,* cit., 1996, pp. 145 y 153. Dictamen AVPD CN10-005, 10 de marzo de 2010, también se refiere a las funciones esenciales para concluir qué actividades tienen la condición de públicas y justifican la aplicación del artículo 21 LOPD.

[2175] Artículo 5 Ley 2/1974, 13 de febrero de 1974, sobre Colegios Profesionales: "*Corresponde a los Colegios Profesionales el ejercicio de las siguientes funciones, en su ámbito territorial: (…)*

i. Ordenar en el ámbito de su competencia la actividad profesional de los colegiados, velando por la ética y dignidad profesional y por el respeto debido a los derechos de los particulares y ejercer la facultad disciplinaria en el orden profesional y colegial. (…)

k. Procurar la armonía y colaboración entre los colegiados, impidiendo la competencia desleal entre los mismos. (…)

m. Intervenir, en vía de conciliación o arbitraje, en las cuestiones que, por motivos profesionales, se susciten entre los colegiados.

n. Resolver por laudo, a instancia de las partes interesadas, las discrepancias que puedan surgir sobre el cumplimiento de las obligaciones dimanantes de los trabajos realizados por los colegiados en el ejercicio de la profesión. (…)

médicos estén llevando a cabo estas actividades se encontrarán realizando funciones de carácter público.

En ocasiones la realización de esas actividades exige el acceso a cierta información sanitaria. Especialmente en el ejercicio de la función disciplinaria, cuando se trata de resolver si un profesional ha incumplido sus obligaciones como tal[2176], será necesario acceder a los datos sanitarios con el fin de aclarar los hechos sucedidos. Cabe preguntarse si estos accesos pueden llevarse a cabo sin el consentimiento del titular de los datos, en aplicación de la excepción que se está analizando.

Podría entenderse que la excepción tiene aplicabilidad aquí por estar así dispuesto en las leyes. El Código de Ética y Deontología Médica parece que abre la puerta a que pueda romperse el deber de secreto de los profesionales sanitarios, sin necesidad de obtener el consentimiento del titular de los datos, cuando comparecen ante el Colegio[2177]. Esta previsión podría tener también justificación en la Ley de Colegios Profesionales, que faculta a dichos entes para que lleven a cabo las ya citadas actividades colegiales de interés público. Podría entenderse que, si la Ley habilita a los Colegios para desarrollar esas actuaciones, y si para llevarlas a cabo las mismas es necesaria la comunicación de datos, será aplicable la excepción al consentimiento por determinación de una Ley, cuestión analizada con anterioridad.

Sin embargo, esta interpretación no se corresponde con la lectura que se ha hecho de la excepción al consentimiento por prescripción legal. Y es que en la citada Ley reguladora de las instituciones colegiales no se prevé cesión de datos alguna, y mucho menos se reconoce la necesidad u obligatoriedad de llevar a cabo ninguna transmisión. Hay que advertir que estas normas fueron aprobadas hace años, cuando la protección de datos no constituía una materia de

---

t. Cumplir y hacer cumplir a los colegiados las Leyes generales y especiales y los Estatutos profesionales y Reglamentos de Régimen Interior, así como las normas y decisiones adoptadas por los Órganos colegiales, en materia de su competencia"; Artículo 3 RD 1018/1980, 19 de mayo de 1980, por el que se aprueban los Estatutos Generales de la Organización Médica Colegial y del Consejo General de Colegios Oficiales de Médicos: "*Fines de la Organización Médica Colegial.*
Son fines fundamentales de la Organización Médica Colegial:
1. La ordenación, en el ámbito de su competencia, del ejercicio de la profesión médica, la representación exclusiva de la misma y la defensa de los intereses profesionales de los colegiados, todo ello sin perjuicio de la competencia de la Administración pública por razón de la relación funcionarial.
2. La salvaguarda y observancia de los principios deontológicos y ético-sociales de la profesión médica y de su dignidad y prestigio, a cuyo efecto le corresponde elaborar los códigos correspondientes y la aplicación de los mismos.
3. La promoción, por todos los medios a su alcance, de la constante mejora de los niveles científico, cultural, económico y social de los colegiados, a cuyo efecto podrá organizar y mantener toda clase de instituciones culturales y sistemas de previsión y protección social.
4. La colaboración con los poderes públicos en la consecución del derecho a la protección de la salud de todos los españoles y la más eficiente, justa y equitativa regulación de la asistencia sanitaria y del ejercicio de la medicina, así como cuantos corresponde y señala la Ley de Colegios Profesionales" y artículo 63: "*Los colegiados incurrirán en responsabilidad disciplinaria en los supuestos y circunstancias establecidas en este estatuto*". CALVO SÁNCHEZ, *Régimen jurídico de los Colegios…,* cit., 1998, p. 621

[2176] MARTÍN-RETORTILLO BAQUER, "El papel de los Colegios…", cit., 1996, p. 335.

[2177] Artículo 16 Código de Ética y Deontología Médica, 1999: "*Con discreción, exclusivamente ante quien tenga que hacerlo, en sus justos y restringidos límites y, si lo estimara necesario, solicitando el asesoramiento del Colegio, el médico podrá revelar el secreto en los siguientes casos: (…)*
f. Cuando comparezca como denunciado ante el Colegio o sea llamado a testimoniar en materia disciplinaria".

especial preocupación. En conclusión, las previsiones legales no son claras a la hora de determinar si la cesión de datos sanitarios a los colegios profesionales requiere del consentimiento del titular o no.

A falta de previsión legal, interesa analizar si la excepción es aplicable en atención al artículo 21 de la LOPD. Como se ha visto, la aplicación de este precepto en el ámbito sanitario está sujeta a una interpretación atendiendo al principio de finalidad. La excepción entra en juego cuando se da dentro del mismo ámbito material. Es decir, en la medida en que la cesión se produce con la finalidad de mejorar el servicio sanitario, y siempre atendiendo al principio de proporcionalidad, se podrá justificar la aplicación de la excepción. En este sentido no parece que sea difícil interpretar que la actividad disciplinaria de los colegios citados repercute en beneficio de un mejor servicio sanitario. No se puede obviar que con esta actividad se determina cuál es el comportamiento considerado adecuado o correcto de los profesionales sanitarios. Parece claro que esta función es de indudable interés público. La propia normativa reconoce que es así. Es por ello por lo que se entiende que la excepción citada puede ser aplicada en este supuesto. Y de igual manera, la excepción será aplicable en los demás casos en que se pueda estimar que la actuación del colegio correspondiente responde a motivos vinculados con la protección y promoción de un sistema sanitario.

En todo caso, habrá que tener en cuenta que la aplicación de la excepción no será automática, sino que tendrá que venir precedida de un previo ejercicio de ponderación en que se valoren diferentes elementos. Habrá que buscar el equilibrio entre la importancia que puede tener esa cesión en la resolución del procedimiento pertinente, y las características y relevancia de la información que se pretende comunicar en relación a los derechos a la intimidad y autodeterminación informativa.

I.5.3. La cesión de datos sanitarios para la salvaguarda de la salud individual y colectiva.

Corresponde ahora analizar el supuesto de cesión que más interés despierta cuando se hace referencia a los datos sanitarios. Se trata de los casos en que estos datos se comunican con la finalidad de proteger la salud. Para llevar a cabo este estudio será necesario aclarar primero cuáles son las normas que se refieren a esta concreta excepción y cuál la relación entre ellas. Una vez fijado este punto será necesario interpretar este marco normativo para determinar cuál es el alcance de la excepción.

I.5.3.A. Identificación de las normas que regulan este supuesto de cesión de datos sanitarios.

Tal y como se ha ido apuntando a lo largo de este capítulo, la cesión de datos sanitarios constituye uno de los puntos de análisis más problemáticos en lo que corresponde al tratamiento de este tipo de información. Se han visto hasta ahora diferentes excepciones recogidas en la normativa reguladora de la protección de datos de carácter personal, aplicables a este tipo de información. No obstante, las excepciones que se han analizado no respondían expresamente a motivos de salud, ni siquiera a motivos concretos, sino que se fundamentaban en disposiciones que se referían a la comunicación de datos en términos genéricos. Lo que ahora se va a analizar es el supuesto en que la cesión responde a motivos de salud. Se trata del supuesto más lógico

de transmisión de estos datos, ya que el uso principal que se da a los mismos es el que se produce en el ámbito estrictamente sanitario.

Son muchos los accesos que se realizan sobre las historias clínicas de las personas. En ocasiones estos accesos se llevan a cabo por parte de sujetos que no pertenecen al ámbito sanitario, sin embargo, la mayoría de ellos son realizados por personal vinculado a este sector. Las cesiones entre diferentes centros, ambulatorios y otras instituciones como puede ser el Gobierno, central o autonómico, o entre los propios profesionales pertenecientes a divisiones distintas con funciones diferentes, son constantes para llevar a cabo la finalidad de proteger la salud de los ciudadanos. Piénsese en este supuesto: a un paciente al que le corresponde acudir a un médico perteneciente a la unidad de atención de su comarca se le diagnostica una patología que requiere de un medicamento específico. Este medicamento se dosifica en otro centro por otros profesionales especializados. Para realizar dicha dosificación será necesario que tengan acceso a determinados datos sanitarios. Por otro lado, si esta enfermedad contiene algún parámetro que pueda afectar a la salud pública, la información deberá transmitirse a la Dirección del Gobierno correspondiente competente en la materia, para realizar los estudios pertinentes. Además otra comunicación será necesaria para realizar los estudios de seguimiento de los efectos del medicamento, de farmacovigilancia. También deberá cederse cierta información a la División de gestión económica para que se realice el control de gastos pertinente. Por último, podría ser necesario realizar una transmisión a la Administración estatal e incluso a determinados organismos de la UE o de la OMS, dependiendo del alcance del riesgo que plantea la enfermedad para la salud pública. Fuera ya del ámbito sanitario, podría pasar que el tratamiento médico fuera defectuoso y que el paciente muriera. Los familiares podrían solicitar la responsabilidad de la Administración correspondiente o del propio profesional sanitario acudiendo a la vía administrativa o judicial. Atendiendo a la relevancia del caso, podría suceder incluso que los medios de comunicación sacaran a la luz determinados datos del paciente.

Todas estas acciones o circunstancias recogen situaciones en que se ceden o transmiten datos sanitarios. Los supuestos en que esta información puede salir del ámbito sanitario, caso del acceso por Jueces y Tribunales o por medios de comunicación, serán analizados más adelante. Ahora se tratará de determinar cómo pueden comunicarse los datos relativos a la salud en el campo estrictamente sanitario.

La LOPD, en la única referencia expresa a la cesión de los datos de salud, dispone que no será necesario el consentimiento "*cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica*"[2178]. La interpretación de este precepto ha de hacerse de acuerdo a lo que diferentes normas han dispuesto sobre la cuestión que se analiza.

[2178] Artículo 11.2.f) LOPD.

El RDLOPD otorga un sentido más amplio a la excepción, señalando que, conforme a lo dispuesto en la normativa sanitaria, no se requerirá el consentimiento del titular para la cesión de datos de salud cuando la finalidad sea la prestación de atención sanitaria[2179].

La Directiva europea no destina ningún artículo concreto a la regulación de la cesión de datos sanitarios por motivos de salud. No obstante, refiriéndose a la información denominada sensible, dispone que no se requiere el consentimiento del titular para el tratamiento de categorías especiales de datos, cuando dicha manipulación sea necesaria para la prevención o el diagnóstico médicos, para la prestación de asistencia sanitaria, para el tratamiento médico o para la gestión de servicios sanitarios, siempre y cuando estas operaciones sean llevadas a cabo por profesionales sujetos al deber de secreto[2180].

La Recomendación del Consejo de Europa dedicada a regular el tratamiento de datos médicos hace referencia expresa a esta cuestión. Según este texto los datos sanitarios sólo pueden comunicarse a personas sujetas al secreto profesional. Los datos médicos se transmitirán sin el consentimiento del titular, siempre y cuando sean relevantes y la cesión esté prevista por una Ley, si constituye una medida necesaria en una sociedad democrática, por razones de salud pública; o, cuando la comunicación está permitida por la Ley, con la finalidad de proteger al sujeto titular de los datos o a un pariente suyo en línea genética, o para proteger un interés vital del titular de los datos o de un tercero. Más allá de estos supuestos, señala la recomendación que se pueden ceder los datos sanitarios si son relevantes y, sentado que el afectado o su representante legal o la autoridad, persona u órgano previstos por la ley no se ha opuesto explícitamente a cualquier comunicación no obligatoria, cuando los datos han sido recogidos en un contexto de prevención, diagnóstico o terapia libremente elegidos, y el propósito de la comunicación, en particular si se trata de la prestación de cuidado al paciente o del funcionamiento de un servicio médico que trabaje en interés del paciente, no es incompatible con el fin del procesamiento para los que los datos fueron recogidos[2181].

La normativa sanitaria estatal también recoge supuestos de cesión de datos sanitarios, que no requirieren del consentimiento del titular de la información, con el fin de proteger la salud tanto colectiva como individual. En relación al primer ámbito señala la LBAP que los ciudadanos tienen el derecho a conocer los problemas de salud que afectan a la colectividad[2182].En algún momento

[2179] Artículo 10.5 RDLOPD: *"Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.*
En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud"

[2180] Artículo 8.3 Directiva. 95/46/CE: "*Por otro lado, no hay que olvidar que la norma europea dispone que no es necesario el consentimiento para el tratamiento de las categorías especiales de datos, cuando el tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicha manipulación se lleve a cabo por profesionales sujetos al deber de secreto".*

[2181] Artículo 7.3 R (97) 5.

[2182] Artículo 6 LBAP: "*Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley*".

estos problemas pueden conllevar la necesidad de dar a conocer datos sanitarios referentes a determinadas personas. También desde este primer punto de vista se permite el acceso por profesionales a la historia clínica con la finalidad de llevar a cabo estudios epidemiológicos, investigaciones, o con fines de protección de la salud pública, siempre y cuando la identificación de los titulares de los datos no sea posible. Si esta finalidad requiere que los datos aparezcan asociados a una persona identificada o identificable será necesario el consentimiento del titular[2183].

Desde un punto de vista individual dispone la LBAP que la historia clínica de cada individuo se realizará de acuerdo a criterios de unidad[2184]. La norma realiza una apuesta clara por la historia clínica única[2185]. En relación a esta herramienta se señala que es el instrumento fundamental para garantizar una asistencia adecuada al paciente. Los profesionales sanitarios deben tener acceso a este documento para poder llevar a cabo su labor[2186]. En lo que afecta a la historia clínica de las personas fallecidas, señala la Ley que tendrán acceso a la misma los sujetos vinculados a ellas por razones familiares o de hecho, salvo que el fallecido hubiese rechazado expresamente esa posibilidad. Sin embargo, parece que se podrá acceder a esas historias clínicas cuando la salud de una persona esté en juego, siempre y cuando dicho acceso se limite a la información estrictamente necesaria[2187]. Se hace una referencia concreta al acceso de los informes de alta señalando que tanto los pacientes como sus familiares o personas

[2183] Artículo 16.3 LBAP: *"El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso".*

[2184] Artículo 15.4 LBAP: "*La historia clínica se llevará con criterios de unidad e integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial*".

[2185] DA Tercera LBAP: "*El Ministerio de Sanidad y Consumo, en coordinación y con la colaboración de las Comunidades Autónomas competentes en la materia, promoverá, con la participación de todos los interesados, la implantación de un sistema de compatibilidad que, atendida la evolución y disponibilidad de los recursos técnicos, y la diversidad de sistemas y tipos de historias clínicas, posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente, en evitación de que los atendidos en diversos centros se sometan a exploraciones y procedimientos de innecesaria repetición*".

[2186] Artículo 16.1 LBAP: "*La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia*".

[2187] Artículo 18.3 LBAP: "*El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.*
Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros".

vinculadas a ellos tienen derecho a recabar el informe de alta donde consta información sanitaria relevante[2188], una vez haya finalizado el proceso asistencial[2189].

En el ámbito autonómico la normativa más reciente ha apostado por dar un sentido amplio a la excepción al consentimiento cuando los datos se emplean en el ámbito sanitario con la finalidad de proteger la salud. Concretamente, se hace depender la aplicabilidad de este límite del hecho de que las comunicaciones se realicen con el objetivo de dar una asistencia sanitaria adecuada al paciente[2190].

En relación a ámbitos más concretos, en la normativa sanitaria pueden encontrarse referencias genéricas a la cesión de datos de salud. La normativa que regula las investigaciones a realizar sobre el cuerpo humano, caso de los ensayos clínicos o las investigaciones biomédicas, exige en todo caso el consentimiento del titular para comunicar la información recabada de dichas operaciones[2191]. Podría entenderse que no cabe la posibilidad de emplear los datos recogidos de las investigaciones citadas, independientemente de la finalidad, sin autorización del titular. No parece que esta interpretación sea acorde a lo que disponen la LBAP o la LOPD. Atendiendo a estas últimas leyes se observa que dependiendo de la finalidad son justificables excepciones al consentimiento del titular. No debe haber problema para comprender que las excepciones aplicables al tratamiento de datos sanitarios puedan emplearse también en estos ámbitos concretos.

I.5.3.B. Sobre la necesidad de realizar una interpretación que favorezca el flujo de información en el ámbito de la sanidad.

Como se acaba de ver, diferentes normas reconocen supuestos en que por motivos de salud pueden llevarse a cabo cesiones de datos sanitarios sin necesidad del consentimiento del titular. De todo este complejo normativo hay que realizar una lectura conjunta. No se pueden llevar a cabo interpretaciones aisladas de los diferentes preceptos. La necesidad de realizar esta

[2188] Artículo 3 LBAP: "*(...) Informe de alta médica: el documento emitido por el médico responsable en un centro sanitario al finalizar cada proceso asistencial de un paciente, que especifica los datos de éste, un resumen de su historial clínico, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas*".

[2189] Artículo 20 LBAP: "*Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3. Las características, requisitos y condiciones de los informes de alta se determinarán reglamentariamente por las Administraciones sanitarias autonómicas*".

[2190] Artículo 5 Decreto 29/2009, 5 de febrero, de Galicia, por el que se Regula el Uso y Acceso a la Historia Clínica Electrónica: *"En particular, no será necesario el consentimiento de la persona interesada para la comunicación de datos personales sobre la salud a través de medios electrónicos, entre organismos, centros, servicios y establecimientos de la Consellería de Sanidad, el Servicio Gallego de Salud y el sistema nacional de salud, cuando se realice para llevar a cabo la atención sanitaria de las personas, tanto se realice con medios propios o concertados*".

[2191] Artículo 3.6 RD 223/2004, 6 de febrero, por el que se Regulan los Ensayos Clínicos con Medicamentos: "*El tratamiento, comunicación y cesión de los datos de carácter personal de los sujetos participantes en el ensayo se ajustará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal, y constará expresamente en el consentimiento informado*". Artículo 5 Ley 14/2007, 3 de julio de 2007, de Investigación Biomédica: "*2. La cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado. En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados*".

interpretación conjunta encuentra base en las remisiones que tanto la normativa sanitaria[2192], como la reguladora de la protección de datos[2193], se hacen mutuamente. De esta manera se podrá llegar a entender la excepción que se comenta de manera más amplia de lo que en un inicio parece sugerir la LOPD.

De una interpretación literal de esta Ley resultan dos supuestos en que se impone la necesidad de salvaguardar la salud de las personas al derecho a la autodeterminación informativa. En principio estos casos aparecen perfectamente delimitados en la norma. La excepción al consentimiento del titular a la hora de llevar a cabo una cesión de datos entra en juego, cuando la cesión responde a una situación de urgencia o es necesaria para realizar los estudios epidemiológicos que se estimen necesarios[2194].

En algún caso se ha interpretado que en este precepto se recoge una única excepción, que requiere de la existencia de un supuesto de urgencia y de la realización de un estudio epidemiológico. Se entendería que es necesario que se produzcan los dos requisitos simultáneamente para que la excepción pueda aplicarse[2195]. Esta interpretación, se considera aquí, carece de base legal, pues la utilización en la disposición de la conjunción "o" deja claro que se trata de dos supuestos exceptuados y no uno sólo: solucionar una urgencia "o" realizar estudios epidemiológicos.

No obstante, la principal interrogante no está en deducir si de este precepto se desprenden una o dos excepciones, sino en saber si más allá de lo dispuesto en esta norma pueden reconocerse otros casos en que se limita el derecho a consentir la cesión de datos sanitarios con el fin de salvaguardar la salud de las personas. La jurisprudencia no ha llevado a cabo una interpretación de este precepto de la LOPD y tampoco la doctrina ha entrado a valorar en profundidad su alcance.

Se entiende aquí que la referencia en la Ley a los estudios epidemiológicos es adecuada, pues amplía la posibilidad de aplicar la excepción a los casos en que está en juego no sólo la salud individual, sino también la colectiva. No obstante, es criticable la referencia expresa a los supuestos de urgencia. Esta expresión reduce el campo de aplicación del artículo cuando se trata de proteger la salud individual a supuestos aislados, que según la legislación sanitaria concernirían sólo a los casos en que la situación clínica del paciente obliga a una atención sanitaria inmediata[2196]. Para los demás supuestos sería necesario el consentimiento del titular.

[2192] Artículo 16 LBAP.
[2193] Artículo 8 LOPD.
[2194] Artículo 11.2.f) LOPD.
[2195] BUISÁN GARCÍA, "Comunicación de datos…", cit., 2008, p. 307: "la cesión de dichos datos si que requiere, en cambio, el consentimiento del afectado salvo, precisamente, en el supuesto contemplado en el presente apartado, cuya aplicación, según resulta de la propia literalidad del precepto, requiere la existencia de dos presupuestos de concurrencia simultánea: que se trate de una situación de urgencia, y que la comunicación sea necesaria para la realización de estudios epidemiológicos".
[2196] Artículo 15 Ley 16/2003, de 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: *"La atención de urgencia se presta al paciente en los casos en que su situación clínica obliga a una atención sanitaria inmediata. Se dispensará tanto en centros sanitarios como fuera de ellos, incluyendo el domicilio del paciente, durante las 24 horas del día, mediante la atención médica y de enfermería"*.

Se plantea la duda, por lo tanto, de si el precepto de la LOPD ha de aplicarse en términos literales o si es posible una interpretación más amplia.

Desde el punto de vista del principio de proporcionalidad podría parecer conveniente que la aplicación de la excepción se limitase exclusivamente a los casos previstos por la Ley. Sólo podría alegarse la excepción en situaciones determinadas en que el sujeto se encontrara en cierto estado de gravedad. Este criterio, sin embargo, se enfrenta a diversos problemas. En primer lugar, a la necesidad de concretar cuándo una situación es urgente. Es innegable que se trata de un concepto muy ambiguo, que dependiendo del criterio científico de cada profesional puede variar. Y en segundo lugar, al hecho de que puede haber situaciones que no son urgentes pero que requieren de la aplicación de la excepción. Piénsese en el caso de un sujeto que tiene una dolencia y llega al centro sanitario en estado de embriaguez, sin que pueda dar un consentimiento consciente. O en el supuesto de un enfermo crónico, que no está en una situación de urgencia pero que requiere de atención constante. Hay que tener en cuenta, además, que las excepciones al consentimiento no sólo han de aplicarse a situaciones en que por cuestiones de tiempo o por incapacidad del titular de los datos éste no pueda otorgarlo, sino también a determinados casos en que el paciente quiere oponerse a una concreta manipulación de sus datos. Estas excepciones salvarían dicha oposición al entender que el derecho a la protección de la salud es merecedor de mayores garantías que el derecho a la autodeterminación informativa.

Se entiende aquí que el criterio de urgencia no es adecuado desde el punto de vista práctico y que hubiera sido conveniente establecer un sistema más flexible a la hora de interpretar la excepción. Atendiendo a esta necesidad de establecer un criterio más flexible, en algún caso se ha interpretado que el consentimiento se requerirá siempre que sea posible[2197]. Es decir, siempre que las circunstancias lo permitan se ha de recoger el consentimiento del titular para llevar a cabo la cesión de datos sanitarios. Si bien en un principio este criterio pudiera parecer asumible, resulta excesivamente ambiguo y no establece parámetros lo suficientemente precisos. Al final se estaría dejando a los profesionales sanitarios la capacidad de decidir cuándo se ha de recabar el consentimiento y cuándo no.

Tratar de establecer un criterio definitivo en el ámbito de la sanidad para fijar cuándo se debe exigir el consentimiento del titular es realmente complicado. Ya se ha dicho que la multitud de situaciones diferentes que se pueden dar en la práctica hace que sea difícil marcar pautas definitivas de actuación. En este sentido tanto la interpretación literal de la Ley como la que lleva a entender que siempre que sea posible se ha de requerir el consentimiento, pueden encontrar acogida en la LOPD. No obstante, en casos dudosos, sería el profesional sanitario el que acabaría determinando si es posible o necesario solicitar la autorización para realizar la cesión de datos. Más allá de la inseguridad que esta situación podría generar entre los profesionales, el

[2197] TRONCOSO REIGADA, *Protección de Datos…* cit., 2008, p. 86: "En todo caso, si bien están vigentes algunos supuestos para la comunicación de datos de salud en virtud de los art. 11 y 21 LOPD, esto no suprime el esfuerzo por alcanzar un consentimiento expreso o una habilitación legal clara para el tratamiento de datos de salud, especialmente cuando se trate de finalidades no asistenciales, como es el caso de las cesiones de datos a la Seguridad Social y a la Administración Tributaria".

dejar en sus manos la determinación del ámbito de aplicación de un límite a un derecho fundamental como el derecho a la autodeterminación informativa no parece ajustado a Derecho.

Se entiende que al interpretar el precepto que se comenta se ha de tener en cuenta la realidad sanitaria. Por un lado, la medicina actual, tan especializada[2198], se presta a que haya más cesiones para cumplir con la finalidad de proteger la salud de las personas[2199]. La especialización hace que tengan que ser más los profesionales, provenientes de divisiones o campos de actuación diferentes, que participen en el proceso asistencial. Hay que tener en cuenta que en la actualidad el trabajo en equipo va más allá del trabajo entre médicos, incluyendo también a personal administrativo que ha de tener acceso, en cierta medida, a los ficheros[2200]. Por otro lado, la cantidad de instancias y órganos que dirigen su actividad en la Administración a la protección de la salud hace que el flujo de información haya de ser mayor. Por último, la actividad sanitaria requiere de múltiples tipos de comunicaciones que, en último término, repercuten en la prestación de un mejor servicio. Un mero cambio de médico, o cambio de hospital[2201], podría requerir de una cesión de datos. Un simple cambio en el sistema de gestión informática de las historias clínicas también puede requerir esta manipulación, caso de la centralización de las historias clínicas. La necesidad de recabar el consentimiento de cada paciente para llevar a cabo estas operaciones obstaculizaría, en todo caso, la agilidad que requiere la práctica sanitaria.

De la realidad expuesta se pueden extraer ejemplos reales que sirven de soporte a un criterio más flexible que el que se desprende del artículo 11 de la LOPD. En el caso del cambio de médico, por ejemplo, el traslado de la historia clínica de un paciente de un profesional a otro puede darse por voluntad del propio paciente, caso en que se entiende que el consentimiento ha sido otorgado para que la transmisión se haga efectiva. Sin embargo, han reconocido los tribunales que incluso cuando la transmisión del expediente no es voluntaria sino forzosa el traslado de la historia puede llevarse a cabo sin el consentimiento del titular[2202]. Es de advertir que en todo caso deberá respetarse el derecho del paciente a elegir el médico que quiera[2203].

[2198] La especialización ha sido puesta de manifiesto por las propias normas. Ejemplo de ello es el artículo 9, 44/2003 21 de noviembre de 2003, de ordenación de las Profesiones Sanitarias: "*La atención sanitaria integral supone la cooperación multidisciplinaria, la integración de los procesos y la continuidad asistencial, y evita el fraccionamiento y la simple superposición entre procesos asistenciales atendidos por distintos titulados o especialistas*".

[2199] DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 157.

[2200] MORENA PÉREZ, "Secreto Médico…", cit., 2000, pp. 127-128; DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 158: "A esta situación, ya de por sí compleja, ha venido a sumarse la problemática generada por lo que ha dado en llamarse secreto médico derivado, surgido a raíz de la medicina institucional y de la compleja organización administrativa de los hospitales actuales que, a partir de actividades como la organización de archivos, bancos de datos o información progresiva, han permitido que personal ajeno al equipo médico acceda a datos sanitarios, como es el caso de administrativos, documentalistas o informáticos".

[2201] SÁNCHEZ-CARO y ABELLÁN, *Datos de Salud...,* 2004, cit., p. 55, se refieren a esta excepción diciendo que "tal regulación impide adoptar soluciones razonables a problemas tan cotidianos como los cambios de hospital, por lo que no parece fácilmente asumible un criterio tan rígido".

[2202] ATC, 11 de diciembre de 1989, se concluye que "ni el derecho a la intimidad de los pacientes ni la relación de confianza entre éstos y sus médicos ha quebrado por el sólo hecho de que los datos médicos e historiales clínicos que obren en un servicio público, como es el Centro Municipal de Planificación Familiar, hayan de continuar en el mismo aunque se preste por otros profesionales distintos".

[2203] Artículo 10.13 LGS: "*Todos tienen los siguientes derechos con respecto a las distintas administraciones públicas sanitarias. 13.A elegir el médico y los demás sanitarios titulados de acuerdo con las condiciones contempladas en esta*

Otro ejemplo lo constituye el proceso de centralización de las historias clínicas dentro de un sistema sanitario. La transmisión de las historias clínicas a una única base de datos requiere de la comunicación de esos documentos al órgano que será el responsable de dicho fichero. La creación del programa denominado Osabide en el País Vasco suponía el traslado de las historias clínicas desde cada unidad asistencial de atención primaria a un único fichero o una única base de datos[2204]. En el sistema sanitario vasco este proceso de centralización produjo un serio debate en el que se planteó la necesidad o no de solicitar el consentimiento de cada uno de los pacientes. Dejando a un lado el transfondo político que subyacía en dicha controversia[2205], puesto de manifiesto en el propio Parlamento vasco[2206], el argumento jurídico fundamental empleado para mostrarse contrario a la creación de esa base de datos era que no se había solicitado el consentimiento de los titulares de los datos para llevar a cabo las pertinentes cesiones requeridas para crear el fichero. En última instancia la centralización se llevó a cabo sin recabar dicha autorización. La Consejería de Sanidad, basándose en sendos informes jurídicos[2207], consideró que las cesiones de las historias clínicas dirigidas a crear la base de datos se realizaban con la finalidad de proteger la salud de los ciudadanos. Esta finalidad justificaba la excepción al derecho a consentir la comunicación de los datos de los pacientes. Esta conclusión fue en cierta medida refrendada posteriormente por la AEPD en una resolución de especial interés, en la que no se reconoció la vulneración del principio de consentimiento[2208].

El hecho de que en los citados ejemplos se haya admitido la cesión de datos sin necesidad de recabar el consentimiento de los titulares de la información sanitaria transmitida lleva a pensar que es posible una interpretación amplia de la excepción recogida en la LOPD para las cesiones de datos de salud, acorde a lo que dispone esta norma en los demás preceptos y lo establecido en las demás normas citadas, que permita un flujo de información más ágil.

I.5.3.C. Fundamentación jurídica de la interpretación amplia propuesta.

Una lectura sistemática de la LOPD justifica una interpretación amplia de la excepción que se comenta. Si se relaciona el artículo 11.2.f) con el ya comentado 7.6 de la Ley no resulta coherente que los supuestos de cesión en el ámbito sanitario sin consentimiento se limiten exclusivamente a los casos de urgencia.

Este último precepto, como ya se interpretó, exceptúa el consentimiento del titular para el tratamiento de los datos de salud no sólo cuando se da una urgencia, sino también cuando la manipulación de los datos se dirige a la prevención o diagnóstico médicos, la prestación de

Ley, en las disposiciones que se dicten para su desarrollo y en las que regule el trabajo sanitario en los centros de salud".

[2204] OTALORA ARIÑO, "Estrategias de Sistemas…", cit., 2002.

[2205] "Ofensiva del PSE para que se anule la sanción a dos médicos de Sansomendi", *El Correo*, 15 de marzo de 2003; "Algo para recordar", *Gara*, 30 de noviembre de 2003; "Los médicos que rechazan Osabide afirman que rompe la confidencialidad con el paciente. CC.OO lanzará una campaña a nivel nacional contra la centralización de historias clínicas", *El País*, 12 de marzo de 2003.

[2206] Diario de Comisiones del Parlamento Vasco, 23 de mayo de 2002. VII Legislatura, Comisión de Sanidad.

[2207] "Informe jurídico complementario a la exposición realizada por el Consejero de Sanidad durante su comparecencia ante la Comisión de Sanidad del Parlamento Vasco el 23 de mayo de 2002 a fin de dar cuenta del proceso de centralización de los datos de los pacientes recogidos en los centros de salud de Osakidetza", 31 de mayo de 2002

[2208] Resolución AEPD, R/00510/2003, 20 de octubre de 2003, procedimiento AAPP/00001/2003.

asistencia sanitaria, tratamientos médicos o para la gestión de servicios sanitarios. No parece que, siendo la excepción en esta disposición tan amplia, pueda reducirse la aplicación de la limitación del consentimiento en las cesiones de datos a supuestos tan limitados.

Para una adecuada asistencia sanitaria es necesaria una información completa sobre el estado de salud del ciudadano, lo cual lleva a que sea imprescindible recopilar la mayor cantidad de datos posible. Esta recopilación exige que tengan que llevarse a cabo cesiones de datos. El hecho de que estas operaciones tengan como fin la protección de la salud justificará la comunicación de información dentro del ámbito sanitario sin el consentimiento del paciente[2209]. Incluso cuando este último se haya opuesto a la manipulación de datos, como se ha argumentado anteriormente, podría justificarse la excepción. El principio de finalidad vuelve a ser determinante en este sentido. La interpretación del precepto que se analiza ha de realizarse a la luz de esta consideración.

La base legal de esta interpretación puede encontrarse, además de en una interpretación sistemática de la LOPD, en otras normas distintas a la citada Ley. El propio RDLOPD dispone que no se requiere el consentimiento del interesado para la cesión de datos de salud cuando la finalidad sea la *"atención sanitaria"*. No se limita a los supuestos de urgencia, sino que hace una interpretación más amplia que se refiere a toda la atención sanitaria. La letra de la disposición general ayuda a realizar una interpretación más amplia que la prevista por la Ley. A la hora de valorar la importancia de la regulación que realiza el reglamento hay que tener en cuenta que su elaboración ha seguido un largo proceso en que han participado diferentes agentes, destacando la AEPD, que ha jugado un papel fundamental en la redacción del mismo[2210].

La Directiva puede entenderse también en el mismo sentido. La norma europea señala que el tratamiento de los datos que requieren de especial protección, entre los que se encuentran los datos de salud, puede llevarse a cabo sin el consentimiento del titular cuando su manipulación sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicha manipulación se realice por profesionales sujetos al deber de secreto. Dentro del concepto de tratamiento cabe englobar la cesión de datos. Resulta evidente que las referencias a la asistencia, prevención, etc. van más allá de los casos de urgencia.

La Recomendación del Consejo de Europa parece seguir la misma línea interpretativa. Respetando siempre el principio de proporcionalidad, se reconoce la posibilidad de comunicar datos médicos cuando la finalidad es la salvaguarda de la salud pública o la protección del sujeto titular de los datos o de un tercero. Se concreta, además, que cuando se trata de operaciones destinadas a la prevención o a la asistencia sanitaria se podrán llevar a cabo las cesiones que se estimen oportunas. Cierto es que para algunos supuestos se matiza que estas operaciones podrán realizarse siempre que no haya habido una oposición expresa del titular de los datos o su representante. No obstante, el hecho de que para estas cesiones se admita el consentimiento

[2209] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 40.
[2210] ORTEGA GIMÉNEZ, "Breve aproximación…", cit., 2007.

tácito es indicativo de la relajación que sufre el derecho a la autodeterminación informativa cuando se trata de proteger la salud de las personas.

La justificación de esta forma de comprender la excepción no sólo se basa en la normativa reguladora de la protección de datos, sino que tiene también su fundamento en la normativa sanitaria interna. Por un lado la creación a nivel estatal por la LBAP de la historia clínica única es indicativo de ello[2211]. Este instrumento evita que haya información sanitaria sobre los ciudadanos dispersa por las distintas entidades que componen el sistema sanitario, entendido en el sentido más amplio. El reparto competencial que entre las diferentes administraciones territoriales llevan a cabo la CE y los Estatutos de Autonomía en materia sanitaria[2212], y la propia organización que las diferentes comunidades autónomas establecen para su sistema sanitario propio[2213], hacen

[2211] DA Tercera LBAP.

[2212] Artículo 149.1 CE: "*El Estado tiene competencia exclusiva sobre las siguientes materias:*
16. Sanidad exterior. Bases y coordinación general de la sanidad. Legislación sobre productos farmacéuticos"; Artículo 148.1 CE: "*Las Comunidades Autónomas podrán asumir competencias en las siguientes materias:*
21. Sanidad e higiene". Junto a la Constitución, los estatutos concretan las competencias que corresponde en materia sanitaria a cada Comunidad Autónoma. Artículo 18 LO 3/1979, 18 de diciembre, Estatuto de Autonomía del País Vasco: "*1. Corresponde al País Vasco el desarrollo legislativo y la ejecución de la legislación básica del Estado en materia de sanidad interior.*
2. En materia de Seguridad Social corresponderá al País Vasco: a) El desarrollo legislativo y la ejecución de la legislación básica del Estado, salvo las normas que configuran el régimen económico de la misma; b) La gestión del régimen económico de la Seguridad Social.
3. Corresponderá también al País Vasco la ejecución de la legislación del Estado sobre productos farmacéuticos. (...)".

[2213] Piénsese en el caso de la CAPV, donde el sistema sanitario alcanza a diferentes administraciones, que a su vez cuentan con órganos distintos que llevan a cabo sus propias funciones. En el caso del Gobierno Vasco, el Departamento de Sanidad y Consumo cuenta con diferentes órganos que dirigen su actividad a proteger la salud de los ciudadanos y que cuentan con sus propios ficheros, como se puede observar en el Registro de la AVPD. Artículo 2 Decreto 579/2009, de 3 de noviembre, por el que se establece la estructura orgánica y funcional del Departamento de Sanidad y Consumo: "*1. (...) el Departamento de Sanidad y Consumo se estructura en los siguientes órganos: A) Órganos centrales: a) Consejero de Sanidad y Consumo (...). b) Viceconsejería de Sanidad. b.1. Dirección de Salud Pública; b.2. Dirección de Aseguramiento y Contratación Sanitaria; b.3 Dirección de Farmacia. c) Viceconsejería de Calidad, Investigación e Innovación Sanitaria (...). B) Órganos periféricos: d) Direcciones Territoriales del Departamento de Sanidad y Consumo: d.1. Álava, d.2. Bizkaia, d.3. Gipuzkoa.*
2. Se encuentran en la situación de dependencia o vinculación, que legalmente corresponda en cada caso, con el Departamento de Sanidad y Consumo los siguientes entes: a) El Ente Público Osakidetza-Servicio Vasco de Salud (...); c) La Fundación Vasca de Innovación e Investigación Sanitaria (...)".
Por su parte, el Ente Público Osakidetza cuenta también con una composición compleja en la que se encuentran órganos diferentes con sus propios ficheros. Artículo 7 Ley 8/1997, 26 de junio, de Ordenación Sanitaria de Euskadi: "*La planificación sanitaria tendrá como base principal de ordenación territorial la división de todo el territorio de la Comunidad Autónoma de Euskadi en las demarcaciones geográficas denominadas áreas de salud, que serán delimitadas reglamentariamente de acuerdo con la situación socio-sanitaria, de manera que puedan ponerse en práctica en su respectivo ámbito los principios y objetivos que enumera esta ley, así como las actuaciones esenciales que requieren la tutela general de la salud pública y la asistencia sanitaria primaria y espeicializada*"; Artículo 1 Decreto 59/2003, de 11 de marzo, por el que se determinan las Áreas de Salud de la Comunidad Autónoma de Euskadi: *De conformidad con lo dispuesto en el artículo 7 de la Ley 8/1997, de 26 de junio, de Ordenación sanitaria de Euskadi, el territorio de la Comunidad Autónoma de Euskadi se divide en tres demarcaciones geográficas denominadas Área de Salud de Álava, de Bizkaia y de Gipuzkoa*". Artículo 1.1 Decreto 195/1996, de 23 de julio, sobre Estructura Organizativa de los recursos adscritos a Osakidetza/Servicio Vasco de Salud para la Atención Primaria: "*Para la gestión asistencial de la Atención Primaria adscrita a Osakidetza/Servicio Vasco de Salud, las Áreas Sanitarias podrán contar bajo la dependencia jerárquica del Director de Área con las siguientes unidades asistenciales y de gestión: a) la Comarca Sanitaria de Atención Primaria, que asumirá en su demarcación territorial y con su respectiva planificación inferior en Unidades e Atención Primaria, las prestaciones sanitarias de asistencia sanitaria y las demás prestaciones de carácter comunitario que se determinen. b) Otras unidades asistenciales y de gestión, que pudieran establecerse para el desarrollo de nuevas prestaciones de Atención Primaria o aquellas que por*

que existan innumerables órganos, departamentos e, incluso, administraciones dedicadas a la causa sanitaria. Si cada una de estas entidades se dedicara individualmente y de manera aislada a la creación de información sobre los usuarios, sin contar con las demás instituciones, se acabarían generando diferentes ficheros sobre las mismas personas con informaciones duplicadas y, lo que podría ser más peligroso, contradictorias. La historia clínica única viene a evitar que esto suceda. Parece evidente que para que este instrumento sea viable será necesario un flujo de información constante que posibilite la puesta en común de todos los datos sanitarios relativos a cada uno. La historia clínica única requiere de comunicaciones de datos sanitarios, más allá de los supuestos de urgencia. Un flujo de información ágil entre las diferentes administraciones facilita la labor de los profesionales sanitarios y hace que su trabajo sea más eficiente, lo que redunda de manera directa en beneficio de la salud de las personas[2214].

Por otro lado, más allá de la previsión de creación de una historia clínica única, la norma plantea de forma más genérica la posibilidad de excepcionar el derecho a consentir la cesión con la finalidad de proteger la salud, determinando que la finalidad de la historia clínica es la asistencia adecuada a los pacientes. Según esta Ley los profesionales sanitarios de cada centro tienen acceso a dicho documento siempre que lo hagan con la finalidad de proteger la salud de dichos pacientes[2215]. Cierto es que la letra de la norma hace referencia a los profesionales asistenciales del centro, por lo que podría deducirse que los accesos sin consentimiento se limitan a los realizados dentro de cada centro. No obstante, no tiene sentido que si la asistencia ha de llevarse a cabo en otro centro, los profesionales de este último tengan que solicitar el consentimiento del titular de los datos. La propia jurisprudencia, aunque escasa en este sentido, ha considerado que la finalidad de la asistencia sanitaria puede justificar el acceso de los profesionales, independientemente del centro dónde se sitúen, a su historia clínica[2216]. Lo mismo puede deducirse de alguna resolución de la AEPD que habilita la cesión de datos sanitarios entre un centro médico privado concertado y la Administración, basándose en que la finalidad perseguida es la asistencia sanitaria[2217].

---

razones de eficiencia asistencial decidieran individualizarse en ámbitos territoriales iguales o inferiores al Área sanitaria"; Artículo 7 Decreto 195/1996, de 23 de julio, sobre Estructura Organizativa de los recursos adscritos a Osakidetza/Servicio Vasco de Salud para la Atención Primaria: "*1. Las Comarcas Sanitarias de Atención Primaria adscritas a Osakidetza/Servicio Vasco de Salud podrán desarrollar, con objeto de incrementar su eficiencia, su modelo organizativo en base a Unidades de Atención Primaria. 2. Las Unidades de Atención Primaria constituyen unidades organizativas de la asistencia formadas por un conjunto de personas, servicios, tecnologías e infraestructuras orientadas a la eficiencia, calidad y eficacia del proceso asistencia y que cuentan un Plan de Gestión*". En el ámbito estatal, RD 263/2011, 28 de febrero, por el que se desarrolla la Estructura Orgánica Básica del Ministerio de Sanidad, Política Social e Igualdad.

[2214] Dictamen APDCat. CNS 11/2007, concluye que no es necesario el consentimiento de los pacientes para crear la denominada Historia Clínica Compartida en Cataluña, que constituye una red de información dirigida a facilitar la asistencia sanitaria en cualquier centro sanitario de dicho territorio. TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, pp. 1.243-1.244.

[2215] Artículo 16 LBAP. STS 30 de diciembre de 2009, FJ 4, subraya esta idea, señalando que para que un profesional sanitario pueda acceder a una historia clínica con fines que no sean asistenciales deberá contar con autorización. Es el caso en que un médico quiere acceder a historias relativas a pacientes de otro médico.

[2216] SAP de Barcelona, 23 de diciembre, 2004, FFJJ 4 y 5; SAP de Madrid 23 de marzo de 2007, FFJJ 5 y 6, en la que se justifica la revelación de información sanitaria de un paciente por parte de un médico a otro profesional sanitario, con el fin de que éste le auxilie en el proceso asistencial del paciente.

[2217] Informe jurídico AEPD, 0600/2009.

La interpretación que se ha hecho en este punto de la LBAP viene reforzada por la letra de otras normas. En la normativa sanitaria autonómica, en algún caso, se ha reconocido de manera expresa la necesidad de que los profesionales tengan acceso a la historia clínica. La legislación catalana, concretamente, dispone que los profesionales sanitarios "*han de tener*" acceso a la historia clínica[2218]. El empleo de ese verbo es significativo. Se justifica el acceso de los profesionales sanitarios a la historia clínica. En este sentido, y desde un punto de vista práctico, este acceso no es un derecho sino una obligación por cuanto que para llevar a cabo su labor han de tener ese acceso a estos documentos[2219]. En la legislación gallega, por su parte, las cesiones de datos sin consentimiento del titular se justifican por el hecho de que tengan por finalidad la "*atención sanitaria de las personas*"[2220].

Además de la LBAP, otras normas de rango legal establecen también la obligación o la necesidad de transmitir información sanitaria sin que tenga que requerirse el consentimiento del titular de los datos. La creación por Ley del actual sistema de información del Sistema Nacional de Salud exige la comunicación constante de datos de carácter personal sanitario[2221]. Se pretende que sea posible acceder a la información sanitaria de cualquier ciudadano en cualquier punto del Estado. Con este mismo fin, la normativa sanitaria ha impuesto a los centros de las diferentes Comunidades Autónomas que configuran el Sistema Nacional de Salud la obligación de incluir un conjunto mínimo de datos en los distintos informes clínicos que crean, para fomentar así la interoperabilidad entre ellos y poder atender a los ciudadanos, independientemente de si se encuentra o no en el lugar en que residen[2222]. Es evidente que detrás de estas previsiones se sitúa la voluntad del legislador de facilitar la creación de un flujo eficiente de datos sanitarios.

En la misma línea la normativa autonómica también prevé situaciones o herramientas que requieren de la interconexión, fundamentalmente con la Administración del Estado, encontrándose supuestos que promueven la creación de un flujo de información dirigido a favorecer una asistencia sanitaria más eficiente[2223]. Es el caso de las cesiones que pudieran

[2218] Artículo 11.2 Ley 21/2000, de Cataluña, 29 de diciembre del 2000, sobre los Derechos de Información relativos a la Salud, la Autonomía del Paciente y la Documentación Clínica: "*La historia clínica es un instrumento destinado fundamentalmente a ayudar a garantizar una asistencia adecuada al paciente. Con este fin, los profesionales asistenciales del centro que están implicados en el diagnóstico o el tratamiento del enfermo han de tener acceso a la historia clínica*".

[2219] MARTÍ MONTESINOS, PIDEVALL BORRELL, "Accesos a la Historia…", cit., 2004, p. 107.

[2220] Artículo 5 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica: *"En particular, no será necesario el consentimiento de la persona interesada para la comunicación de datos personales sobre la salud a través de medios electrónicos, entre organismos, centros, servicios y establecimientos de la Consellería de Sanidad, el Servicio Gallego de Salud y el sistema nacional de salud, cuando se realice para llevar a cabo la atención sanitaria de las personas, tanto se realice con medios propios o concertados*".

[2221] Artículos 53 a 56, Ley 16/2003, 28 de mayo de 2003, de Cohesión y Calidad del Sistema Nacional de Salud. TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, p. 1.245.

[2222] Exposición de Motivos RD 1093/2010, 3 de septiembre de 2010, por el que se aprueba el Conjunto Mínimo de Datos de los informes clínicos en el Sistema Nacional de Salud: "*Este real decreto, atendidas la diversidad de sistemas y tipos de historias clínicas vigentes en el ámbito de cada comunidad autónoma, y con el consenso de profesionales sanitarios de distintas áreas de conocimiento, pretende establecer el conjunto mínimo de datos que deberán contener una serie de documentos clínicos con el fin de compatibilizar y hacer posible su uso por todos los centros y dispositivos asistenciales que integran el Sistema Nacional de Salud*".

[2223] Artículo 17.1 Decreto 270/2003, 4 de noviembre de 2003, por el que se crea y regula el Registro Vasco de Voluntades Anticipadas: "*El Registro Vasco de Voluntades Anticipadas se interconectará con el Registro Nacional de Instrucciones Previas en los términos previstos en la Ley 41/2002, de 14 de noviembre y su normativa de desarrollo*".

derivar del empleo de las llamadas de urgencia, para las que no se requerirá el consentimiento cuando la situación así lo exija[2224]. Todas estas comunicaciones tienen como fin la salvaguarda de la salud de las personas en situaciones que muchas veces no son de urgencia. Si se interpretara que los datos de salud sólo pueden cederse sin el consentimiento del titular en los supuestos de urgencia, sería prácticamente imposible crear el sistema de información que se propone en las leyes. De todo esto se deduce que estas cesiones pueden realizarse sin necesidad de la autorización del titular[2225].

En el Código de Ética y Deontología Médica puede encontrarse también fundamento a la excepción al derecho a consentir, basado en la protección de la salud de las personas. Se señala en este texto que podrá romperse el deber de secreto de los profesionales sanitarios cuando sea necesario para proteger al propio paciente, titular de los datos, o a otras personas[2226].

Reflejo de la necesidad de asumir una interpretación más amplia que la que en un inicio pueda resultar de una lectura literal de la LOPD son diferentes instrumentos, además de la historia clínica única, que en el día a día se emplean en la práctica sanitaria para la gestión de los diferentes servicios. La utilización de estas herramientas exige un flujo constante de información, que de verse sujeto a la necesidad de recabar autorización de cada uno de los titulares de los datos sanitarios resultaría obstaculizado.

A) Se puede hablar, por ejemplo, de la Tarjeta Sanitaria[2227]. Si la citada historia clínica única requiere la comunicación de los datos sanitarios de los ciudadanos para que puedan ser atendidos en cualquier punto del Estado, el instrumento que ahora se comenta posibilita que estos ciudadanos puedan ser identificados en cualquier lugar, incluso en otro Estado europeo. Como reconocen las normas, la tarjeta sanitaria individual que se pretende implantar exige la transmisión de información[2228]. Las normas exigen que este tipo de operaciones se lleven a cabo

[2224] Artículo 31.3 Ley 9/2007, 30 de julio de 2007, del Centro de Atención y Gestión de Urgencia 112 Cataluña: "*Los ficheros a los que se refiere el apartado 2 deben recoger los datos de carácter personal de los ciudadanos que pidan la prestación del servicio. Dichos ficheros pueden recoger datos protegidos por la legislación vigente, siempre y cuando sean datos cedidos o recaudados voluntariamente, o siempre y cuando sean determinantes de la forma en que debe atenderse la urgencia o prestar la asistencia material requerida*".

[2225] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 120.

[2226] Artículo 16 Código de Ética y Deontología Médica: "*Con discreción, exclusivamente ante quien tenga que hacerlo, en sus justos y restringidos límites y, si lo estimara necesario, solicitando el asesoramiento del Colegio, el médico podrá revelar el secreto en los siguientes casos: (…)*
d. Si con su silencio diera lugar a un perjuicio al propio paciente o a otras personas; o a un peligro colectivo". AAP de Álava 28 de noviembre de 2005, FJ 1.

[2227] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 116-117.

[2228] Artículo 57 Ley 16/2003, 28 de mayo de 2003, de Cohesión y Calidad del Sistema Nacional de Salud: "*1. El acceso de los ciudadanos a las prestaciones de la atención sanitaria que proporciona el Sistema Nacional de Salud se facilitará a través de la tarjeta sanitaria individual, como documento administrativo que acredita determinados datos de su titular, a los que se refiere el apartado siguiente. La tarjeta sanitaria individual atenderá a los criterios establecidos con carácter general en la Unión Europea.*
2. Sin perjuicio de su gestión en el ámbito territorial respectivo por cada comunidad autónoma y de la gestión unitaria que corresponda a otras Administraciones públicas en razón de determinados colectivos, las tarjetas incluirán, de manera normalizada, los datos básicos de identificación del titular de la tarjeta, del derecho que le asiste en relación con la prestación farmacéutica y del servicio de salud o entidad responsable de la asistencia sanitaria. Los dispositivos que las tarjetas incorporen para almacenar la información básica y las aplicaciones que la traten deberán permitir que la lectura y comprobación de los datos sea técnicamente posible en todo el territorio del Estado y para todas las Administraciones públicas. Para ello, el Ministerio de Sanidad y Consumo, en colaboración

en un entorno seguro, cumpliendo con las oportunas medidas de seguridad y controles de acceso[2229]. Las cesiones de datos, sobre todo referentes a la identificación de las personas, son necesarias para que los ciudadanos puedan acceder a los sistemas sanitarios de los diferentes lugares a los que puede acudir, y para que en dichos sistemas puedan acceder, a su vez, a la historia clínica de cada paciente. La necesidad del consentimiento para poder llevar a cabo estas transmisiones ha de ser cuestionada. En primer lugar, la previsión legal parece eximir de la necesidad de recabar el consentimiento del titular para llevar a cabo las cesiones oportunas. En segundo lugar, la necesidad de proteger la salud de las personas que solicitan asistencia en cualquier punto del Estado justifica también estas comunicaciones.

B) La otra herramienta paradigmática en este sentido es la receta electrónica que ya se ha puesto en marcha en algunos territorios y que se ha tratado de definir más arriba[2230]. Este instrumento resulta imprescindible para la dispensación de medicamentos y para el control del uso que de ellos se vaya a realizar.

Resulta básico para una adecuada asistencia sanitaria la correcta dispensación de medicamentos. La receta electrónica facilita esta operación empleando las nuevas tecnologías, que permiten la rápida transmisión de información, lo cual agiliza la labor de los profesionales

con las comunidades autónomas y demás Administraciones públicas competentes, establecerá los requisitos y los estándares necesarios.
3. Con el objetivo de poder generar el código de identificación personal único, el Ministerio de Sanidad y Consumo desarrollará una base de datos que recoja la información básica de asegurados del Sistema Nacional de Salud, de tal manera que los servicios de salud dispongan de un servicio de intercambio de información sobre la población protegida, mantenido y actualizado por los propios integrantes del sistema. Este servicio de intercambio permitirá la depuración de titulares de tarjetas.
4. Conforme se vaya disponiendo de sistemas electrónicos de tratamiento de la información clínica, la tarjeta sanitaria individual deberá posibilitar el acceso a aquélla de los profesionales debidamente autorizados, con la finalidad de colaborar a la mejora de la calidad y continuidad asistenciales.
5. Las tarjetas sanitarias individuales deberán adaptarse, en su caso, a la normalización que pueda establecerse para el conjunto de las Administraciones públicas y en el seno de la Unión Europea".

[2229] Artículo 6 RD 183/2004, 30 de enero, por el que se regula la Tarjeta Sanitaria Individual: "*1. La relación de agentes del sistema sanitario autorizados para el acceso a la base de datos y sus capacidades de operación con esta base serán acordadas por el Consejo Interterritorial del Sistema Nacional de Salud.*
2. Sin perjuicio de las competencias atribuidas a la Agencia Española de Protección de Datos, el Ministerio de Sanidad y Consumo determinará las medidas de índole técnica y organizativa que hayan de imponerse en relación con la base de datos de población protegida del Sistema Nacional de Salud y que sean necesarias para garantizar tanto la seguridad como la disponibilidad de los datos de carácter personal, evitando su alteración, pérdida, tratamiento y, en especial, el acceso no autorizado a aquélla. En todo caso, dichas medidas se atendrán a lo establecido en la legislación vigente en materia de protección de datos personales.
3. El Ministerio de Sanidad y Consumo, como responsable de la base de datos, aplicará las medidas de seguridad y accesos de conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado".

[2230] RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación; Decreto 206/2008, 28 de agosto, de Receta Electrónica, DO de Galicia nº 181, de 18 de septiembre de 2008; Decreto 181/2007, de 19 de junio, por el que se regula la Receta Médica Electrónica, BO de la Junta de Andalucía nº 123, 22 de junio de 2007; Decreto 159/2007, de 24 de julio, por el que se regula la Receta Electrónica y la Tramitación Telemática de la Prestación Farmacéutica a cargo del Servicio Catalán de la Salud, DO de la Generalitat de Catalunya nº 4934, 26 de julio de 2007; Orden 22 de noviembre de 2004, del Consejero de Sanidad, por la que se establecen Normas sobre el Uso de la Firma Electrónica en las relaciones por Medios Electrónicos, Informáticos y Telemáticos con el Sistema Sanitario de Euskadi, BOPV nº 227, de 26 de noviembre de 2004.

que han de llevar a cabo esa dispensa[2231]. Para que médico y farmacéutico puedan ejecutar estas funciones es necesario que se transmitan datos sanitarios de los pacientes[2232]. Más allá de esta transmisión son necesarias otras, dirigidas sobre todo a cumplir con objetivos vinculados a la gestión económica o administrativa, fundamentalmente el control de gastos, y a la vigilancia y evaluación de los productos farmacéuticos. Ya se ha apuntado antes la necesidad de que exista un flujo de información, sobre todo con los órganos del Ministerio de Sanidad y Consumo para cumplir con estos fines[2233]. Estas cesiones se multiplican debido a la complejidad del sistema sanitario que deriva de la estructura autonómica del Estado[2234]. Las leyes concretan la información que las recetas médicas han de contener para cumplir con su función[2235].

[2231] APARICIO SALOM, "Análisis de la normativa…", cit., 2006, p. 285.

[2232] STS 30 de marzo de 1989, FJ 5, incluso la jurisprudencia ha puesto de manifiesto la importancia de esta transmisión de datos.

[2233] Artículo 33.1, Ley 16/2003, 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud: "*Las oficinas de farmacia colaborarán con el Sistema Nacional de Salud en el desempeño de la prestación farmacéutica a fin de garantizar el uso racional del medicamento. Para ello los farmacéuticos actuarán coordinadamente con los médicos y otros profesionales sanitarios"*; Anexo I Decreto 159/2007, 24 de julio, por el que se regula la Receta Electrónica y la Tramitación Telemática de la Prestación Farmacéutica a cargo del Servicio Catalán de la Salud: "*los datos recabados en el Registro de Prestación Farmacéutica se cederán al Consejo General de Farmacéuticos y a las entidades con las que el Servicio Catalán de la Salud hay concertado la prestación de atención farmacéutica, al Departamento de Salud, al Instituto Catalán de la Salud y al Ministerio de Sanidad y Consumo*".

[2234] RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación, recoge los diferentes supuestos de comunicación de datos que requiere la coordinación de los distintos sistemas sanitarios autonómicos, a efectos no sólo de dispensación de medicamentos, sino también con objetivos

[2235] Artículo 3 RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación: "*1. Las recetas médicas, públicas o privadas, pueden emitirse en soporte papel, para cumplimentación manual o informatizada, y en soporte electrónico, y deberán ser complementadas con una hoja de información al paciente, de entrega obligada al mismo, en la que se recogerá la información del tratamiento necesaria para facilitar el uso adecuado de los medicamentos o productos sanitarios prescritos.*

2. El prescriptor deberá consignar en la receta y en la hoja de información para el paciente los datos básicos obligatorios, imprescindibles para la validez de la receta médica, indicados a continuación:

a) Datos del paciente:1.º El nombre, dos apellidos, y año de nacimiento; 2.º En las recetas médicas de asistencia sanitaria pública, el código de identificación personal del paciente, recogido en su tarjeta sanitaria individual, asignado por su Servicio de Salud o por las Administraciones competentes de los regímenes especiales de asistencia sanitaria. En el caso de ciudadanos extranjeros que no dispongan de la mencionada tarjeta, se consignará el código asignado en su tarjeta sanitaria europea o su certificado provisional sustitutorio (CPS) o el número de pasaporte para extranjeros de países no comunitarios. En todo caso se deberá consignar, asimismo, el régimen de pertenencia del paciente.3.º En las recetas médicas de asistencia sanitaria privada, el número de DNI o NIE del paciente. En el caso de que el paciente no disponga de esa documentación se consignará en el caso de menores de edad el DNI o NIE de alguno de sus padres o, en su caso, del tutor, y para ciudadanos extranjeros el número de pasaporte.

b) Datos del medicamento: 1.º Denominación del principio/s activo/s o denominación del medicamento; 2.º Dosificación y forma farmacéutica y, cuando proceda, la mención de los destinatarios: lactantes, niños, adultos; 3.º Vía o forma de administración, en caso necesario; 4.º Formato: número de unidades por envase o contenido del mismo en peso o volumen; 5.º Número de envases o número de unidades concretas del medicamento a dispensar; 6.º Posología: número de unidades de administración por toma, frecuencia de las tomas (por día, semana, mes) y duración total del tratamiento. Los datos referidos en los epígrafes 4.º y 5.º sólo serán de obligada consignación en las recetas médicas emitidas en soporte papel. En las recetas médicas emitidas en soporte electrónico sólo serán de cumplimentación obligada por el prescriptor cuando el sistema electrónico no los genere de forma automática.

c) Datos del prescriptor:1.º El nombre y dos apellidos; 2.º La población y dirección donde ejerza. La referencia a establecimientos instituciones u organismos públicos solamente podrá figurar en las recetas médicas oficiales de los mismos; 3.º Número de colegiado o, en el caso de recetas médicas del Sistema Nacional de Salud, el código de identificación asignado por las Administraciones competentes y, en su caso, la especialidad oficialmente acreditada que ejerza. En las recetas médicas de la Red Sanitaria Militar de las Fuerzas Armadas, en lugar del número de colegiado podrá consignarse el número de Tarjeta Militar de Identidad del facultativo. Asimismo se hará constar, en su caso, la especialidad oficialmente acreditada que ejerza; 4.º La firma será estampada personalmente una vez cumplimentados los datos de consignación obligatoria y la prescripción objeto de la receta. En las recetas electrónicas se requerirá la firma electrónica, que deberá producirse conforme con los criterios establecidos por la

Evidentemente estas transmisiones afectan a la autodeterminación informativa de los pacientes[2236]. No obstante, al igual que ocurría con la tarjeta sanitaria, el ordenamiento, a pesar de encontrarse referencias que apuntan lo contrario[2237], excluye la necesidad de requerir el consentimiento del titular de los datos cuando el empleo de este instrumento tiene por finalidad la asistencia sanitaria[2238]. La Ley que regula el uso de los medicamentos recoge expresamente la excepción a la necesidad de recabar el consentimiento del titular para la cesión de datos sanitarios en el ámbito de uso de la receta electrónica, siempre que la finalidad sea asistencial o de control de la prestación farmacéutica[2239]. Esta normativa reconoce, sin embargo, la necesidad

---

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. En las recetas del Sistema Nacional de Salud, los datos del prescriptor, a los que se refieren los epígrafes 2.º y 3.º se podrán consignar de forma que se garantice la identificación del prescriptor y se permita la mecanización de dichos datos por los servicios de salud y las mutualidades de funcionarios.

d) Otros datos: 1.º La fecha de prescripción (día, mes, año): fecha del día en el que se cumplimenta la receta; 2.º La fecha prevista de dispensación (día, mes, año): fecha a partir de la cual corresponde dispensar la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable; 3.º N.º de orden: número que indica el orden de dispensación de la receta, en el caso de dispensaciones sucesivas de tratamientos crónicos o medicamentos de dispensación renovable. Los datos referidos en los epígrafes 2.º y 3.º sólo serán de obligada consignación en las recetas médicas en soporte papel.

Además de los datos señalados en los epígrafes anteriores, en su caso, deberá ser consignado el visado por las Administraciones sanitarias, de acuerdo con el Real Decreto 618/2007, de 11 de mayo, por el que se regula el procedimiento para el establecimiento, mediante visado, de reservas singulares a las condiciones de prescripción y dispensación de los medicamentos. En caso de recetas electrónicas, el visado se realizará en la forma prevista en el artículo 8.7 de este real decreto.

En las recetas médicas en soporte papel y en la hoja de información al paciente para el caso de receta electrónica se incluirá una cláusula que informe al paciente en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3. La hoja de información para el paciente estará diferenciada de la receta pudiendo ser separable de la misma, o bien constituir un impreso independiente, donde el prescriptor podrá relacionar todos los medicamentos y productos sanitarios prescritos, facilitando al paciente la información del tratamiento completo y el diagnóstico, si procede, a juicio del prescriptor.

4. Todos los datos e instrucciones consignados en la receta médica deberán ser claramente legibles, sin perjuicio de su posible codificación adicional con caracteres ópticos. Las recetas médicas no presentarán enmiendas ni tachaduras en los datos de consignación obligatoria, a no ser que éstas hayan sido salvadas por nueva firma del prescriptor". Artículo 3.1 Decreto 181/2007, 19 de junio, de Andalucía, que regula la Receta Médica Electrónica: *"La receta médica electrónica contendrá los siguientes datos: a) La identificación del prescriptor: nombre, apellidos y código numérico personal. b) La identificación del paciente: nombre, apellidos, edad y número de identificación sanitaria. c) La identificación de la prescripción del medicamento o producto sanitario: 1.º Número de identificación generado por el sistema informático, que será único e irrepetible. 2.º Datos mínimos necesarios para su identificación inequívoca que, a estos efectos, son exclusivamente los que figuran en el catálogo informatizado de medicamentos y productos sanitarios que se pueden prescribir mediante la receta médica electrónica. 3.º Posología y duración del tratamiento. d) Fecha de prescripción"*.

[2236] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 125-126.

[2237] Artículo 8.1 Decreto 159/2007, 24 de julio, que regula la Receta Electrónica y la Tramitación Telemática de la Prestación Farmacéutica a cargo del Servicio Catalán de la Salud: "*Los farmacéuticos y las farmacéuticas de las oficinas de farmacia sólo deben acceder a los datos de los productos incluídos en la prestación farmacéutica prescritos a una persona paciente cuando ésta se identifique y pida su dispensación. Sin embargo, los farmacéuticos y las farmacéuticas de las oficinas de farmacia podrán acceder a los datos de los productos incluidos en la prestación farmacéutica prescritos a una persona paciente para hacer consultas relacionadas con la medicación, a petición de la persona paciente, que deberá dar su autorización expresa, de la que debe quedar constancia, de acuerdo con la normativa vigente*".

[2238] APARICIO SALOM, "Análisis de la normativa…", cit., 2006, pp. 301-306, fundamenta la excepción al consentimiento directamente en el artículo 7.6 LOPD y en la normativa sanitaria.

[2239] Artículo 77.8 Ley 29/2006, 26 de julio de 2006, de Garantías y Uso Racional de los Medicamentos y Productos Sanitarios: "*No será necesario el consentimiento del interesado para el tratamiento y la cesión de datos que sean consecuencia de la implantación de sistemas de información basados en receta médica en soporte papel o electrónico, de conformidad con lo dispuesto en los artículos 7, apartados 3 y 6; 8; y 11, apartado 2.a, de la Ley Orgánica*

de que en cumplimiento de la LOPD toda manipulación y conservación de datos deba realizarse en un ámbito de absoluta seguridad[2240]. En la práctica, tal como señala expresamente alguna norma, los profesionales farmacéuticos sólo tendrán acceso a los datos para la dispensa de medicamentos si el propio paciente facilita la tarjeta sanitaria para que pueda verificarse su identidad y validar la operación[2241]. Esta previsión podría parecer que contradice la regulación expuesta, que exceptúa la necesidad del consentimiento para estos supuestos, pues si es el paciente quien voluntariamente ha de dar la citada Tarjeta al farmacéutico, el acceso será consecuencia de este acto y será por lo tanto consentido. Esta última regulación encuentra justificación por cuanto el acceso a los datos del paciente ha de limitarse al farmacéutico que va a atenderle. La excepción al consentimiento no significa que todos los farmacéuticos tienen libre acceso a la información de un paciente. El empleo de la tarjeta sanitaria implica que sólo el profesional elegido por el paciente para la dispensa tendrá acceso a los datos, sin que sea necesario que otros profesionales lleven a cabo dicho acceso. La necesidad de que el paciente transmita la tarjeta al farmacéutico para la dispensa de medicamentos no resta virtualidad al límite al consentimiento impuesto en el ordenamiento cuando los datos se emplean en el uso de la receta electrónica. Se ha de concluir que esta excepción se refiere a la falta de necesidad de autorización del paciente para que los datos puedan transmitirse por las redes de información para emplear la receta electrónica con fines asistenciales. La finalidad, por lo tanto, determina el alcance del límite al derecho a la autodeterminación informativa.

La habilitación legal en el caso de la receta electrónica parece limitarse a la dispensación de los fármacos. Basándose en este hecho en algún momento se ha entendido que para llevar a cabo la cesión de estos datos empleando la receta electrónica pero con otras finalidades será necesario el consentimiento del titular. Podría ser el caso del servicio farmacoterapéutico, que se ha comprendido como una operación más de gestión que de asistencia dirigida a la protección de la salud de las personas[2242]. Efectivamente, para estas operaciones no hay previsión legal que exceptúe la exigencia del consentimiento del titular de los datos a la hora de llevar a cabo la cesión. Es más, en la normativa autonómica en algún caso se exige dicha autorización

15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Las citadas actuaciones deberán tener por finalidad facilitar la asistencia médica y farmacéutica al paciente y permitir el control de la prestación farmacéutica del Sistema Nacional de Salud"; En el mismo sentido artículo 19.2 RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación.TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 132-134.

[2240] Artículos 11, 18 y 19 RD 1718/2010, 27 de diciembre de 2010, sobre Receta Médica y Órdenes de Dispensación.

[2241] Artículo 16 Artículo Decreto 206/2008, 28 de agosto, de Receta Electrónica de Galicia: "*1. Los/as farmacéuticos/as autorizados/as de las oficinas de farmacia sólo tendrán acceso a los datos para la prestación farmacéutica del/ de la usuario/a cuando este/a se identifique con su tarjeta sanitaria, o excepcionalmente con los medios previstos en el artículo 9.2 del presente decreto, y solicite la dispensación de los productos farmacéuticos prescritos (…)*"; 14 Decreto 93/2009, 24 de abril, por el que se regula la implantación de la Receta Electrónica en el Ámbito del Sistema Sanitario Público de Extremadura: "*Los farmacéuticos tendrán acceso a los datos para la prestación farmacéutica cuando el paciente solicite la dispensación de los medicamentos o productos sanitarios prescritos y facilite la tarjeta sanitaria para su inserción y reconocimiento en el Sistema de Información Funcional de Receta Electrónica.*

Asimismo, los farmacéuticos podrán acceder a los datos de los medicamentos y productos sanitarios incluidos en la prestación farmacéutica prescritos a un paciente para efectuar consultas relacionadas con la medicación siempre que el paciente facilite la tarjeta sanitaria para su inserción y reconocimiento en el citado sistema".

[2242] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 129-131.

expresamente[2243]. Sin embargo, el que la farmacoterapia sea considerada como una disciplina dirigida exclusivamente a la gestión administrativa puede ser puesto en duda. El seguimiento farmacoterapéutico es un ejercicio indispensable en el que interaccionan paciente y farmacéutico con el fin de dispensar un servicio farmacéutico adecuado a las necesidades de cada paciente. Así lo han dispuesto también las normas[2244]. Cabe preguntarse si, a pesar de no contar con una previsión legal al respecto, la excepción no puede venir fundada en la finalidad que se persigue con la farmacoterapia. Y es que con esta actividad se busca también la salvaguarda de la salud de las personas. Va más allá del control en la dispensa del medicamento. Se trata de analizar la evolución del paciente con respecto a los medicamentos que haya podido consumir. Es obvio que este ejercicio repercute en la salud de las personas. Así, en la medida en que el fin es la protección de la salud, podría pensarse que, cuando menos en los supuestos en que las leyes no obliguen a lo contrario, cualquier cesión de datos que pudiera dirigirse a hacer efectiva esta actividad no requerirá del consentimiento del titular.

En conclusión, la regulación vigente da base suficiente para reconocer que el derecho a consentir una cesión de datos puede verse limitado cuando la finalidad de dicha operación es la asistencia sanitaria directa de las personas. Dejando atrás una interpretación restrictiva de la letra de la LOPD, se entiende aquí que la protección de la salud constituye un bien jurídico suficiente para limitar el derecho a consentir. En este caso la finalidad que se persigue es la que justifica la aplicación de la limitación. En apartados anteriores se ha visto la posibilidad de exceptuar el derecho a consentir por determinación de la Ley o por llevarse a cabo las cesiones entre distintas administraciones. En este supuesto, el hecho de que la manipulación de datos se dirija a la protección de la salud constituye el argumento que justifica la excepción. Se ha analizado en el capítulo tercero cómo ha de interpretarse esta finalidad y el alcance que tiene como bien jurídico que justifica el límite al consentimiento. Sin embargo, no hay que olvidarlo, a pesar de que el derecho a consentir pueda verse limitado, los demás principios y derechos que integran la autodeterminación informativa quedan plenamente vigentes. La aplicación de los principios de calidad recogidos en el artículo 4 LOPD llevará, por ejemplo, a que sólo determinados profesionales puedan tener acceso a los datos de cada paciente con el fin de proteger su salud. No todos los profesionales sanitarios han de tener acceso a la totalidad de historias clínicas, sino sólo quienes asisten a cada paciente. Este argumento ha sido puesto de manifiesto por el TEDH en relación a un supuesto en que gran parte de los profesionales que trabajaban en un centro conocían el estado de salud de una determinada paciente[2245]. También ha sido empleado por las agencias de protección de datos para subrayar que el personal de

[2243] Artículo 17.2 Ley 19/1998, 25 de noviembre de 1998, de Ordenación y Atención Farmacéutica de la Comunidad de Madrid.

[2244] Artículo 17 Ley 19/1998, 25 de noviembre de 1998, de Ordenación y Atención Farmacéutica de la Comunidad de Madrid: "*1. Se entiende por seguimiento farmacoterapéutico el realizado con el registro sistemático de la terapia medicamentosa de un paciente, con el objetivo de detectar, prevenir y reparar problemas relacionados con los medicamentos, tales como incumplimiento del tratamiento, duplicaciones terapéuticas, errores de prescripción, reacciones adversas, interacciones y contraindicaciones*"

[2245] STEDH 17 de julio de 2008, I v. Finlandia, FFJJ 35-49.

enfermería deberá tener acceso a la historia clínica únicamente en la medida en que sus funciones lo requieran, sin aceptar una facultad de acceso generalizado[2246].

I.5.3.D. Supuestos concretos de cesiones de datos sanitarios dirigidos a proteger la salud de las personas.

I.5.3.D.a. Las cesiones de datos sanitarios en beneficio de familiares, allegados y otros terceros.

En los supuestos analizados hasta ahora, la cesión de datos de salud se realizaba dentro del ámbito estrictamente sanitario entre los profesionales, con la finalidad de llevar a cabo una asistencia eficiente con respecto a una persona determinada, que era la titular de los datos. Sin embargo, la comunicación de estos datos puede darse también a favor de otros sujetos con la finalidad de proteger la salud, o bien del paciente, o bien de terceros. La mayoría de estos casos se refieren a cesiones realizadas a familiares o allegados del titular de los datos, para proteger la salud de este último o la de esas terceras personas familiares o allegadas.

En relación a estas cesiones la LGS establecía de manera genérica el derecho de los familiares o allegados a que se les dé en términos comprensibles información completa y continuada sobre el proceso asistencial, incluyendo diagnóstico, pronóstico y alternativas de tratamiento[2247]. Se les cedía a estos sujetos la historia clínica sin necesidad de que se recabara la autorización del titular de los datos. Esta facultad reconocida a estos sujetos no puede ser aceptada hoy día desde la perspectiva del derecho a la autodeterminación informativa[2248]. Así, la nueva LBAP dispone que los familiares serán informados en la medida que el paciente lo permita de forma expresa o tácita[2249].

Se entiende que, de acuerdo a la normativa vigente, no puede establecerse de manera genérica un derecho de los familiares y allegados a conocer la información sanitaria de un paciente. Esta posibilidad atentaría contra el derecho a la autodeterminación informativa y la intimidad. La jurisprudencia ha sancionado en algún supuesto la entrega de datos sanitarios al familiar de un paciente, sin haber recabado su consentimiento[2250]. En principio, tiene que ser el paciente el que determine si quiere que éstos conozcan la información sanitaria relativa a su persona. A pesar de que la ley no lo indique expresamente, se entiende que para que el

[2246] Informe jurídico AEPD, 656/2008.
[2247] Artículo 10.4 LGS: se reconoce el derecho de los familiares de los pacientes *"a que se le dé en términos comprensibles, a él y a sus familiares o allegados, información completa y continuada, verbal y escrita, sobre su proceso, incluyendo diagnóstico, pronóstico y alternativas de tratamiento"*.
[2248] SAP Alicante 6 de julio de 2001, FJ 3, afirma que "tampoco es lo mismo la entrega del historial médico al propio paciente, que la entrega realizada a un familiar". BELTRÁN AGUIRRE, Juan Luis, "La Información en la Ley General de Sanidad y en la Jurisprudencia", *DS*, vol. 3 nº 2, 1995, p. 163: haciendo referencia al citado artículo 10.5 de la LGS afirma que "teniendo en cuenta que quien ostenta el derecho a recibir la información es el paciente, no se entiende muy bien por qué a los familiares y, sobre todo, a los allegados –término éste impreciso e indeterminado por demás- se les sitúa en el mismo nivel".
[2249] Artículo 5.1 LBAP: *"El titular del derecho a la información* (asistencial) *es el paciente. También serán informadas las personas vinculadas a él, por razones familiares o de hecho, en la medida que el paciente lo permita de manera expresa o tácita"*.
[2250] SAN 9 de noviembre de 2005, FJ 6.

consentimiento se vea exceptuado será necesario que existan causas que justifiquen esta limitación[2251].

Las cesiones a favor de los familiares o allegados sin el consentimiento del titular pueden darse en distintos supuestos, más allá de los casos de representación legal. A) En primer lugar, la comunicación de datos de un paciente a familiares o allegados suyos puede tener sentido para favorecer una adecuada asistencia. En numerosas ocasiones puede ser de especial utilidad el que los familiares tengan conocimiento de la situación de la salud de una persona, sobre todo a la hora de darle los cuidados adecuados. Así, en muchos casos el profesional sanitario deberá informar a los familiares o personas cercanas sobre su estado de salud aunque no se dé el consentimiento del titular[2252]. Esta circunstancia puede reconocerse por ejemplo, con mucha claridad, en el campo de la psiquiatría[2253]. Muchos de los problemas relacionados con la mente afectan no sólo al individuo que padece la enfermedad, sino también a los sujetos que comparten su entorno más íntimo. El adecuado tratamiento de estas enfermedades requiere de la participación de los sujetos que le rodean. Para que esta participación sea la conveniente será necesario que estas terceras personas tengan acceso a información sanitaria del paciente.

De la misma manera, podrían justificarse también supuestos en que es necesaria la comunicación de datos sanitarios a asistentes sociales o incluso a centros donde se trata a sujetos que precisan de determinados cuidados[2254]. El cuidado de personas ancianas, por ejemplo, exige que los sujetos que van a llevar a cabo esos tratamientos conozcan la situación de la salud de aquéllas. Lo mismo ocurre cuando se trata de un menor que precisa de asistencia social por los problemas de salud de sus padres o por los suyos propios[2255].

B) En segundo lugar, la cesión de datos sanitarios a favor de personas allegadas o familiares puede estar justificada cuando la salud de estos últimos está en juego. Hay ocasiones en que el conocimiento de datos de salud de una persona determinada puede ser necesario para la salvaguarda de la salud de un familiar o allegado. Un supuesto conocido en este sentido puede ser el que se plantea en el caso de las personas afectadas por el VIH. Evidentemente, para la protección de la salud de la persona allegada, e incluso de los profesionales que han de tratarlo, será necesario conocer determinada información sobre la salud de la persona infectada por el

[2251] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 77.
[2252] *European Standards on Confidentiality and Privacy in Healthcare among Vulnerable Patient Populations,* del 8 de Julio de 2005, p. 17.
[2253] MORENA PÉREZ, "Secreto Médico…", cit., 2000, p. 132: "Los tratamientos de pareja o terapia sexual, las terapias de familia y las terapias grupales son ámbitos que comparten el hecho de que lo que en otras terapias se define individualmente, el paciente, aquí está integrado por varias personas (...), lo que implica que la confidencialidad se pueda vulnerar a niveles más complejos".
[2254] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 82. Si bien estas profesiones de carácter social no parecen encontrarse en el ámbito de aplicación de la Ley 44/2003, de 21 de noviembre de 2003, de ordenación de las Profesiones Económicas, no puede negarse que en cierta medida estas actividades tienen indudable repercusión en la salud de las personas; RAMÍREZ NEILA, "Accesos legítimos…", cit., 2009, p. 296.
[2255] STEDH de 27 de agosto de 1997, Anne Marie Andersson v. Suecia,. LÓPEZ AGÚNDEZ, "Cabe la cesión...", cit., 2003. En esta misma línea se ha pronunciado la APDCM la cual ha afirmado que es posible la cesión de datos de salud entre órganos administrativos sin consentimiento del paciente siempre que tenga la finalidad de tutela y protección del menor de edad. Pueden, por lo tanto transmitirse datos sobre el estado de salud de los padres de un menor de edad a la administración en defensa de los intereses del menor.

virus[2256]. Lo mismo ocurre cuando se realizan análisis genéticos a un individuo de los que se deduce cierta información sobre determinados miembros de su familia, como puede ser la propensión a padecer una enfermedad concreta. Si de los datos sanitarios concernientes a una persona puede deducirse información valiosa para la protección de la salud de otra, necesariamente ha de estar permitida la cesión sin consentimiento de dichos datos. Hacer depender esta cesión de la voluntad del sujeto titular de los datos sería hacer depender la salud de esa tercera persona de dicha voluntad. Hay que tener en cuenta, siguiendo el ejemplo que se ha dado, que si no se informa al tercer sujeto de la propensión a sufrir determinada enfermedad no tendrá la posibilidad de prever un tratamiento[2257].

Si bien esto es así, cabe preguntarse si en estos supuestos es necesario que el tercero familiar o allegado tenga acceso directo a la información, o si basta con que lo tengan los profesionales sanitarios que lo van a atender o tratar. En principio no parece que sea indispensable el acceso por esas personas cercanas. Los profesionales sanitarios que tienen conocimiento de determinada información sobre una persona pueden emplear dichos datos para tratar a un tercero, sin que éste conozca la fuente de la información. Siendo así, el principio de proporcionalidad exige que sean los profesionales quienes tengan acceso a la información y no los familiares o allegados.

C) El acceso a la información sanitaria de un paciente por parte de familiares o personas vinculadas a él encuentra apoyo en el articulado de la LBAP, en la regulación de un supuesto muy concreto. Se trata del acceso de estos sujetos a los informes de alta hospitalaria. Señala la norma que tanto los familiares como los allegados tendrán el derecho, en su caso, a recibir el informe de alta correspondiente después de que haya finalizado el proceso asistencial[2258]. Hay que tener en cuenta que el contenido de este informe no es precisamente irrelevante desde el punto de vista de los derechos a la intimidad y autodeterminación informativa. La misma norma recoge que dicho informe especifica los datos del paciente, un resumen de su historia clínica, la actividad asistencial prestada, el diagnóstico y las recomendaciones terapéuticas[2259]. Podría plantearse si es acorde con lo expuesto hasta ahora el que se otorgue a familiares y allegados un acceso ilimitado a dicha documentación.

[2256] MUÑOZ CONDE, *Derecho Penal…*, cit., 2004, pp. 268-269: En relación al caso en que el médico tenga conocimiento de esa afección "si este peligro de contagio es muy grande, por ejemplo, para otro personal médico que se ocupe del tratamiento o o que de algún modo deba tener contacto con el portador, el médico debe advertir de esta situación a las personas en peligro, quedando amparada su revelación bien por la vía del estado de necesidad (primando el derecho a la salud de terceros sobre el derecho a la intimidad del seroportador), bien por la del cumplimiento de un deber de denunciar un delito (en el caso de que el portador contagie o con su conducta pueda contagiar voluntariamente a otros). En algunos casos puede que, por la peculiaridad del ámbito donde se obtiene el dato, el médico tenga obligación de revelarlo al organismo oficial (…) o la empresa para la que trabaja (…)";Esta posición parece compartida, hoy día, por la mayoría de los autores. DE MIGUEL SÁNCHEZ, *Tratamiento de Datos...*, cit., 2004, pp. 119-124; VERDÚ PASCUAL, *Secreto Profesional…,* cit., 2005, p. 70.

[2257] NICOLÁS JIMÉNEZ, *La Protección…,* cit., 2006, p. 282-284.

[2258] Artículo 20 LBAP: "*Todo paciente, familiar o persona vinculada a él, en su caso, tendrá el derecho a recibir del centro o servicio sanitario, una vez finalizado el proceso asistencial, un informe de alta con los contenidos mínimos que determina el artículo 3 (...)*". PELLEJERO GARCÍA, "Informes de Alta…", cit., 2004, p. 297.

[2259] Artículo 3 LBAP.

La jurisprudencia y la doctrina no han entrado a valorar la adecuación de esta regulación. Se entiende aquí, sin embargo, que cuando menos cabe cuestionar su validez. Si se considera que el derecho de acceso de familiares y allegados a la historia clínica completa de un paciente está limitada en la propia LBAP, no se entiende cómo puede justificarse el acceso ilimitado a un documento que recoge el resumen de dicha historia clínica. No es justificable que estos terceros puedan disponer de la intimidad y los datos del paciente de esta manera. En este sentido podría realizarse, partiendo de la letra de la propia Ley, una interpretación acorde a lo dicho hasta ahora. Dispone la Ley que cada uno de los sujetos, paciente, familiar o persona vinculada, tendrá el derecho a recibir el documento "en su caso". Podría interpretarse que el acceso de los terceros al informe no es absoluto sino que, en el caso de los familiares y allegados, podrá producirse sólo en determinadas circunstancias en que no sea el propio titular el que pueda recibir y acceder a dicho documento, o por lo menos, cuando el propio titular no se haya opuesto a dicho acceso.

D) El ordenamiento regula otro supuesto concreto de acceso por terceros familiares o allegados a la información sanitaria de un paciente. Se trata del caso en que éste ha fallecido y las personas vinculadas a él quieren acceder a su historia clínica por razones familiares o de hecho. Dispone la posibilidad de que estos familiares o allegados accedan al documento salvo que el fallecido haya prohibido previamente dicho acceso. Para aquellos terceros que no sean familiares o allegados el acceso a la historia clínica del fallecido se limita a los supuestos en que su salud dependa de dicho acceso[2260]. Se distinguen, por lo tanto, dos figuras distintas: el acceso por parte de los familiares y personas vinculadas a él por razones de hecho, y el acceso por los demás terceros. Este precepto ha sido criticado por disponer un sistema de acceso ilimitado o absoluto a favor de terceras personas a la historia clínica de los fallecidos[2261]. De hecho, en algún momento ha parecido que las agencias de protección de datos han llevado a cabo una interpretación especialmente amplia de esta posibilidad de acceso[2262].

La protección de la información de las personas fallecidas ha sido objeto de debate[2263]. Se ha cuestionado si la regulación dirigida a la protección de datos es aplicable a los fallecidos. Desde una perspectiva general la AEPD ha marcado unos criterios bastante certeros al respecto. La personalidad, según el CC, se extingue con la muerte[2264]. Partiendo de esta consideración, se

[2260] Artículo 18.4 LBAP: *"Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros*".

[2261] ATELA BILBAO, y GARAY ISASI, "Ley 41/2002…", cit., 2004, p. 74.

[2262] Dictamen AVPD CN09-044, 26 de octubre de 2009: "Desde la perspectiva de protección de datos por tanto, las autoridades de control no ven obstáculo alguno al acceso del familiar respecto a los datos sanitarios del fallecido, salvo que se acredite una prohibición expresa de éste, y siempre que dicho acceso no vulnere la intimidad del fallecido, no afecte a las anotaciones subjetivas de los profesionales participantes, ni perjudique a terceros".

[2263] DE MIGUEL SÁNCHEZ, *Secreto Médico…*, 2002, pp. 184-185, señala que para cumplir este fin basta con que los familiares puedan acceder al informe de alta; DE LORENZO Y MONTERO, *Derechos y Obligaciones...,* 2003, p. 120, concluye que la LBAP parece negar la posibilidad de entregar la historia clínica de un fallecido a sus familiares, por cuanto supondría una vulneración de su intimidad.

[2264] Artículo 32 CC: "*La personalidad civil se extingue con la muerte de las personas*".

puede concluir que el derecho a la autodeterminación informativa, siendo personalísimo, se extingue también con la muerte de las personas. Así lo ha entendido la AEPD en diferentes informes jurídicos[2265]. Siguiendo esta línea, en la normativa dirigida a regular la protección de datos de carácter personal, el nuevo RDLOPD dispone que no será de aplicación dicho reglamento a la información concerniente a las personas fallecidas, si bien los familiares o allegados de éstas podrán dirigirse a los responsables de los ficheros o tratamientos con el fin de notificar el óbito y, en su caso, cancelar los datos referentes a estos sujetos[2266]. De lo expuesto se desprende que la normativa reguladora de la protección de datos no es aplicable a la información concerniente a las personas fallecidas. En un principio esta conclusión tiene pleno sentido. Como bien ha señalado la doctrina, los principios que determinan la calidad de los datos obligan, en principio, a que las manipulaciones de información cesen cuando fallezca el titular de los datos[2267]. Normalmente las finalidades que justificaban los tratamientos de datos se agotan con la muerte del titular de los datos. Por otro lado, difícilmente puede ejercerse el control de los datos por la persona, sobre todo cuando se trata de ejercer los derechos de acceso, cancelación y rectificación, si ésta ha fallecido[2268]. Estas consideraciones llevan a la conclusión de que, en general, la protección de los datos de las personas se extingue con su fallecimiento. Sin embargo, se ha de realizar un apunte a esta afirmación. Según determinadas leyes la protección del derecho a la intimidad, al honor y a la propia imagen va más allá de la muerte de los sujetos[2269]. Se pueden ejercer acciones dirigidas a proteger estos derechos, incluso una vez que el sujeto titular de los mismos haya fallecido. No se está diciendo que estos derechos perduren más allá de la muerte de las personas, cosa discutida incluso por la jurisprudencia[2270], sino que su protección puede ejercerse más allá de la muerte de las personas[2271]. Hay que recordar que el derecho a la protección de datos tiene por objeto, especialmente, salvaguardar los derechos al honor y a la intimidad personal y familiar[2272]. De este modo, en la medida en que las acciones para proteger dichos derechos pueden perdurar más allá de la muerte de las personas, y las acciones para proteger el derecho a la autodeterminación informativa se dirigen a la salvaguarda de aquéllos, parece correcto afirmar que la autodeterminación informativa perdura a pesar de la

[2265] Informe jurídico de la AEPD, 365/2006, "Tratamiento y cesión de datos de personas fallecidas"; Informe jurídico de la AEPD, 61/2008, "Aplicación de las normas de protección de datos a los datos de personas fallecidas"; Informe jurídico de la AEPD, 278/2009, "Cesión de datos de personas fallecidas, exclusión de la aplicación de la LOPD".

[2266] Artículo 2.4 RDLOP: "*Este Reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos*".

[2267] PUENTE ESCOBAR, "Comentario al artículo…", cit., 2008, p. 53.

[2268] Informe jurídico AEPD de 23 de mayo de 2003.

[2269] Artículo 6.1 LO 1/1982, 5 de mayo de 1982, de Protección Civil del Derecho al Honor, a la intimidad Personal y Familiar y a la Propia Imagen: "*Cuando el titular del derecho lesionado fallezca sin haber podido ejercitar por sí o por su representante legal las acciones previstas en esta Ley, por las circunstancias en que la lesión se produjo, las referidas acciones podrán ejercitarse por las personas señaladas en el artículo cuarto*".

[2270] STC 12 noviembre de 1990, FJ 4: "la información, al margen de su veracidad o falsedad, lesionó de manera ilegítima el honor y la intimidad personal del piloto fallecido".

[2271] GÓMEZ RIVERO, *La Protección…,* cit., 2007, p. 137. TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, p. 1.121.

[2272] Artículo 1 LOPD.

muerte de las personas, cuando menos en cuanto es medio indispensable para proteger los citados derechos[2273].

La afirmación de que el derecho a la autodeterminación informativa se extingue con la muerte podría llevar a la conclusión de que el acceso a la historia clínica de las personas fallecidas por parte de terceras personas no encuentra obstáculo ninguno. Se podría plantear que los datos sanitarios contenidos en ese documento pasan a ser de acceso público. Esta afirmación se contradice con lo dispuesto en la LBAP, que limita el acceso por parte de terceros a las historias clínicas de los fallecidos a determinados supuestos. La remisión que la LOPD realiza a la normativa sanitaria para la regulación de los datos sanitarios justifica que, a pesar de que pudiera reconocerse cierta contradicción entre las normas, la regulación de la LBAP sea directamente aplicable[2274].

En principio, reconoce la Ley la posibilidad de que las personas familiares o allegadas al fallecido puedan acceder a la historia clínica de ésta cuando argumenten razones familiares o de hecho. Este acceso puede limitarse si la persona fallecida deja antes de su muerte constancia de su voluntad de que ningún familiar o allegado pueda acceder a esa información sanitaria. El problema que plantea esta regulación es la dificultad que puede encontrarse en la práctica a la hora de acreditar esta prohibición. Como ha señalado la doctrina, no son comunes los casos en que un sujeto haya prohibido el acceso a su historia clínica a sus familiares y allegados antes de su muerte[2275]. De esta forma, no se puede exigir a los centros un esfuerzo desproporcionado a la hora de averiguar si hay constancia de esa prohibición y normalmente deberán ser los propios familiares de la persona fallecida los que deberán aportar pruebas al respecto[2276]. Más allá de este problema, se plantea la duda de si esta prohibición es absoluta, o si cuando el acceso responde a motivos determinados puede relajarse. Se entiende aquí que cuando la salud de las personas allegadas o familiares esté en juego esta prohibición puede ser exceptuada. Si durante todo este apartado se ha ido afirmando que el derecho a la autodeterminación informativa ha de ceder en beneficio de la protección de la salud, habrá que interpretar que la citada prohibición puede salvarse cuando la salud de personas vinculadas al fallecido está en juego. En caso de que esa prohibición no existiera, los citados sujetos podrán acceder a la historia clínica[2277].

Cuando se quiere acceder a la historia clínica de la persona fallecida en beneficio de un tercero no vinculado por razones familiares o de hecho el acceso a la información sanitaria aparece más limitado: sólo se dará cuando esté en juego la salud de estos terceros[2278]. En este caso la Ley no establece limitación alguna al acceso por motivos de salud. La cesión de los datos al tercero se da independientemente de que se trate de una situación de urgencia o no, siempre y cuando esté en juego la salud de un sujeto.

[2273] Informe jurídico "Acceso a los datos de una persona fallecida obrantes en un determinado expediente de servicio de ayuda a domicilio", *Datospersonales.org,* nº 29, 28 de septiembre de 2007.
[2274] Resoluciones de la AEPD, R/00560/2008, 19 de mayo de 2008, procedimiento TD/00040/2008; R/00629/2009, 30 de marzo de 2009, procedimiento TD/01576/2008.
[2275] ATELA BILBAO, y GARAY ISASI, "Ley 41/2002…", cit., 2004, p. 74.
[2276] Dictamen APDCat. CNS 28/2009.
[2277] SÁNCHEZ-CARO y ABELLÁN, *Datos de Salud...*, 2004, p. 46.
[2278] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 78-79; DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 120.

En estos últimos casos, tanto cuando lo que está en juego es la salud de una persona cercana, como cuando se trata de la salud de otra persona, ocurre lo mismo que lo comentado más arriba sobre el acceso a la información sanitaria de una persona no fallecida en beneficio de un tercero. Se plantea la duda sobre si el acceso ha de realizarse por los propios terceros o por los profesionales que los van a tratar. Como se decía entonces, el principio de proporcionalidad exige que el acceso lo lleven a cabo los profesionales, pues no es necesario para cumplir el fin citado que los terceros, sean familiares o no, conozcan los datos relativos a la salud de la persona fallecida. A pesar de que la normativa citada se refiere al acceso directo del tercero, no parece que este acceso sea, de inicio, necesario.

I.5.3.D.b. Las cesiones de datos sanitarios con la finalidad de salvaguardar la salud pública.

I.5.3.D.b.a´. Referencia a la posible contradicción entre las normas que regulan este supuesto.

El análisis realizado hasta ahora se ha dirigido a estudiar los supuestos en que se protege la salud individual de las personas, bien sea del titular de los datos, personas vinculadas a él o terceros. No obstante, la cesión de datos puede beneficiar no sólo a la salud de una persona, sino también a la sociedad en general[2279]. La protección de la salud integra un componente colectivo de gran importancia. La salvaguarda de esta salud pública o colectiva requiere también de la cesión de datos sanitarios[2280].

Es función de la Administración velar por la salud pública y garantizar el derecho a la protección de la salud que la CE reconoce a los ciudadanos. Uno de los instrumentos principales que se emplea en cumplimiento de este objetivo es la investigación. Se ha señalado que la Constitución reconoce el derecho a la investigación y reclama a los poderes públicos la promoción de esta actividad[2281]. Interesa aquí la investigación en el ámbito de la sanidad y, dentro de este tipo de actividad el estudio epidemiológico. El ordenamiento se ha hecho eco de la necesidad de esta última herramienta[2282]. En la actualidad, a la vista de situaciones como las generadas por el que se ha conocido coloquialmente "síndrome de las vacas locas" o la reciente gripe aviaria, estos estudios se plantean también a escala europea e incluso mundial[2283].

[2279] DÍAZ MÉNDEZ, "La Historia…", cit., 2000, p. 53.
[2280] MEDRANO ALBÉNIZ, "El secreto…", cit., 2000, pp. 14-15.
[2281] Artículos 20.1.b) y 44.2 CE.
[2282] RD 2214/1995, de 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica; Artículo 6 LBAP: "*Derecho a la información epidemiológica. Los ciudadanos tienen derecho a conocer los problemas sanitarios de la colectividad cuando impliquen un riesgo para la salud pública o para su salud individual, y el derecho a que esta información se difunda en términos verdaderos, comprensibles y adecuados para la protección de la salud, de acuerdo con lo establecido por la Ley"*; Real Decreto, 711/2002, de 19 de julio, por el que se regula la Farmacovigilancia de Medicamentos de Uso Humano, en su artículo 5.c) recoge como función de la Agencia Española del Medicamento "*promover la creación de bases de datos sanitarias informatizadas que sirvan como fuente de información para la realización de estudios farmacoepidemiológicos"*.
[2283] En la Decisión relativa a la Posición Común aprobada por el Consejo con vistas a la adopción de la Decisión del Parlamento Europeo y del Consejo por la que se crea una Red de Vigilancia Epidemiológica y de Control de las Enfermedades Transmisibles en la Comunidad Europea, DO nº C 034 del 2 de febrero de 1998, se plantea la necesidad de "crear una red a escala comunitaria para potenciar la cooperación y la coordinación entre los Estados Miembros, con la asistencia de la Comisión, a fin de mejorar la prevención y el control en la Comunidad de las categorías de

La realización de las investigaciones puede llevarse a cabo directamente sobre el cuerpo de los pacientes, o accediendo a información ya contenida en un sistema sanitario determinado. En el primer caso, como se vio en el capítulo dedicado al consentimiento, el ordenamiento exige, la mayoría de veces, la autorización del titular para recabar información y realizar las investigaciones oportunas[2284]. Interesa ahora analizar si el mismo criterio se sigue cuando la información se recaba no directamente del propio titular, sino accediendo a ficheros que ya cuentan con los datos.

En la mayoría de ocasiones, para llevar a cabo esta labor investigadora y de tratamiento epidemiológico resulta necesaria la transmisión de datos de carácter personal sanitarios[2285]. Es imprescindible que determinados órganos de diferentes administraciones y profesionales sanitarios ajenos a la asistencia sanitaria accedan a la información. Ejemplo de ello es uno de los mecanismos más importantes que se emplean para llevar a cabo las investigaciones y estudios epidemiológicos, como es el Conjunto Mínimo Básico de Datos (CMBD), que constituye una base de datos de contenido médico y administrativo relativa a las personas que se han sometido a un episodio de hospitalización y a la que se tiene acceso con el fin de recabar información para realizar desde evaluaciones de calidad de un sistema sanitario concreto hasta investigaciones. La creación de esta base de datos está sujeta a constantes cesiones de datos entre diferentes órganos y administraciones.

La cuestión a analizar es si esta transmisión requiere el consentimiento de los titulares de los datos que se pretenden manipular. Adelantando la conclusión que se defiende, la cesión de datos para desarrollar este tipo de estudios se realizará, en muchos casos, sin necesidad de recabar el consentimiento del afectado. El ordenamiento es confuso en relación a esta cuestión. La LBAP exige que los datos que se empleen con el fin de llevar a cabo estudios epidemiológicos no puedan vincularse con la identidad de sus titulares[2286]. Se requiere, por lo tanto, su

enfermedades transmisibles especificadas en el anexo". La red "se establecerá poniendo en contacto permanente, mediante todos los medios técnicos apropiados, a la Comisión y a las estructuras y/o autoridades que, en cada Estado miembro y bajo la responsabilidad del mismo, tengan competencia a escala nacional y se encarguen de recabar la información relativa a la vigilancia epidemiológica de las enfermedades transmisibles, estableciendo procedimientos para la difusión a escala comunitaria de los datos oportunos en materia de vigilancia". En el mismo sentido la Posición Común (CE) nº 32/97 aprobada por el Consejo el 22 de julio de 1997 con vistas a la adopción de la Decisión nº .../97/CE del Parlamento Europeo y del Consejo, por la que se crea una Red de Vigilancia Epidemiológica y de Control de las Enfermedades Transmisibles en la Comunidad, considera que "*para garantizar la protección de la población en caso de situación de urgencia, los Estados miembros deben intercambiar, sin demora, a través de la red comunitaria, los datos e informaciones pertinentes"*.

[2284] SÁNCHEZ CARAZO, *La intimidad…,* cit., 2000, p. 205.

[2285] ÁLVAREZ CIENFUEGOS, *La Defensa...*, 1999, cit., p. 115; VELÁZQUEZ BAUTISTA, *100 interrog@ntes...*, cit., 2004, p. 35.

[2286] Artículo 16.3 LBAP; "*El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso*"; Artículo 17.4 LBAP: "*La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y*

anonimización. Este requisito sólo podrá levantarse en caso de que se cuente con el consentimiento del titular de los datos. Partiendo de esta regulación no se permite en esta norma el tratamiento de datos de carácter personal sin el consentimiento del titular con la finalidad citada. En algún caso esta posición ha parecido tener apoyo en la doctrina y en algún informe de la AEPD[2287]. Sin embargo, desde el mismo ámbito sanitario se han mostrado argumentos contrarios a esta regulación inicial. Por un lado, la importancia que la LGS otorga a la actuación preventiva y a la necesidad de que se cree un sistema de información que permita una adecuada realización de estos estudios se contrapone a la citada regla establecida en la LBAP para el tratamiento de los datos de salud con este fin[2288]. Desde el ámbito autonómico, normas dirigidas a regular la protección de la salud pública han habilitado la posibilidad de emplear datos sanitarios sin necesidad de recabar el consentimiento del titular[2289]. Pueden encontrarse en este ámbito autonómico, sin embargo, otros ejemplos que han adoptado la posición contraria a la que se acaba de citar[2290]. Por otro, fundamentalmente, investigadores han afirmado que tratar de proteger con especial celo la autodeterminación informativa de los pacientes puede llevar a obstaculizar la realización de las investigaciones[2291].

La LOPD recoge una regulación distinta a la prevista en la LBAP. La Ley de protección de datos realiza una referencia expresa a la cesión de datos de salud en la que dispone que no será necesario el consentimiento del titular para llevar a cabo cesiones con el fin de llevar a cabo estudios epidemiológicos[2292]. Además, en relación al principio de finalidad, señala que el empleo

funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas".

[2287] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, pp. 87-88. Informe jurídico de la AEPD, "Cesión de datos de salud para fines de investigación", 0509/2009. En el mismo sentido Dictamen APDCat. CNS 18/2010, en la que se analiza la posibilidad de ceder datos sanitários con el fin de llevar a cabo un estúdio sobre la morbilidad de determinado colectivo profesional, o Dictamen APDCat. CNS 9/2010.

[2288] Artículo 8 LGS: "*1. Se considera como actividad fundamental del sistema sanitario la realización de los estudios epidemiológicos necesarios para orientar con mayor eficacia la prevención de los riesgos para la salud, así como la planificación y evaluación sanitaria, debiendo tener como base un sistema organizado de información sanitaria, vigilancia y acción epidemiológica*".

[2289] Artículo 10 Ley 18/2009, 22 de octubre, de Salud Pública de Cataluña: "*3.Todas las administraciones públicas y los organismos competentes en materia de salud pública, así como todos los centros, servicios y establecimientos sanitarios y los profesionales sanitarios, deben participar, en el ámbito de sus funciones respectivas, en el Sistema de Formación e Investigación en Salud Pública y en el Sistema de Información de Salud Pública. A tal fin, deben comunicar a estos sistemas los datos pertinentes mediante sus órganos responsables.*

4. Los datos de carácter personal que las personas físicas y jurídicas a que se refiere el apartado 3 recojan en el ejercicio de sus funciones pueden cederse, de acuerdo con lo establecido por el artículo 11.2.a de la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, para que la Agencia de Salud Pública de Cataluña los trate para desarrollar el Sistema de Información de Salud Pública y el Sistema de Formación e Investigación en Salud Pública, así como con finalidades históricas, estadísticas o científicas en el ámbito de la salud pública. Sin embargo, la cesión de datos de historias clínicas para que la Agencia de Salud Pública de Cataluña los trate para desarrollar las funciones del Sistema de Información de Salud Pública y el Sistema de Formación e Investigación en Salud Pública requiere la disociación previa de los datos que permitan identificar la persona titular, salvo que esta haya dado previamente su consentimiento a la cesión, de acuerdo con lo establecido por la normativa reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínicas".

[2290] Artículo 8 Decreto 89/1999, 10 de junio, por el que se regula el Conjunto Mínimo Básico de Datos (CMBD) al alta hospitalaria y cirugía ambulatoria, en la Comunidad de Madrid: *"En los casos en los que se necesite utilizar datos de carácter personal para alguna investigación relacionada con este fichero se realizará con datos disociados, y si no pudieran ir disociados, se le pedirá el consentimiento expreso al ciudadano para poder utilizar sus datos con este fin*".

[2291] DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 292.

[2292] Artículo 11.2.f) LOPD.

de unos datos con fines históricos, estadísticos o científicos no es incompatible con la finalidad que justificó en un principio la recogida de dichos datos[2293]. Puede interpretarse que cualquier dato, independientemente del objetivo que motivó su recogida, puede ser empleado posteriormente con fines científicos. En la misma línea que la Ley, la recomendación del Consejo de Europa dedicada a la protección de datos médicos señala que la comunicación de estos datos podrá darse sin el consentimiento del titular con el fin de proteger la salud pública, cuando una Ley así lo prevea y sea necesaria[2294]. Los órganos judiciales también han puesto de manifiesto en alguna ocasión de manera expresa la necesidad de que la cesión de datos de carácter personal, incluso los sensibles, se pueda dar sin el consentimiento del titular cuando se dirijan a cumplir la finalidad que ahora se analiza[2295].

Parece clara la contradicción inicial entre la normativa sanitaria y la referente a la protección de datos. Para salvarla es necesario realizar una interpretación conjunta de todas las normas que entran en juego. Se trata de buscar una solución intermedia a las planteadas por las leyes citadas.

Como punto de partida no se asume aquí la regulación de la LBAP como definitiva. No se puede obviar la importancia que tienen los estudios epidemiológicos en el ámbito sanitario, sobre todo para la prevención de enfermedades. En ocasiones las investigaciones y los estudios epidemiológicos constituyen actividades urgentes, debido a su importancia en un momento determinado para proteger la salud de la ciudadanía. Además, a este hecho hay que sumarle que con frecuencia las investigaciones requieren de información relativa a un número alto de sujetos, lo que precisa de un esfuerzo desproporcionado para recabar el consentimiento de dichas personas. Exigir ese consentimiento en estos casos podría obstaculizar gravemente la realización de esta actividad[2296].

I.5.3.D.b.b´. Justificación y alcance de la excepción al consentimiento cuando la finalidad del tratamiento de datos es la realización de estudios epidemiológicos y otras investigaciones.

Si bien es cierto que el principio de proporcionalidad y la normativa sanitaria exigen que cuando sea posible los datos sean tratados anónimamente y con el consentimiento del titular, no puede dejar de reconocerse la posibilidad de que en determinadas circunstancias sea necesario el tratamiento de los datos sanitarios con el citado fin sin consentimiento.

[2293] Artículo 4.2 LOPD.
[2294] Artículo 7.3.a.i) R (97) 5.
[2295] STSJ de la Comunidad Valenciana de 27 de noviembre del 2002, FJ 2, señala que "la prohibición de tratamientos automatizados de datos de carácter íntimo referidos a la salud o a la sexualidad de las personas, contiene una excepción, cuando los mismos sean utilizados por una Administración Pública en defensa de intereses colectivos, como son la evitación de la propagación y transmisión de enfermedades contagiosas, pero siempre que estos datos sean utilizados para estos fines y con las garantías que la propia Ley Orgánica 5/92 establece en la regulación del tratamiento automatizado de datos". En el mismo sentido la SAN de 24 de marzo de 2004, FJ. 6 reconoce que no es necesario el consentimiento del titular de los datos cuando la cesión de estos datos es necesaria para la salvaguarda de un interés colectivo, en este caso la salud pública. Así, en los FFJJ 8 y 9, justifica la creación de un fichero relativo al Sistema de información sobre nuevas infecciones, y la posibilidad de manipular datos de carácter personal para realizar estudios epidemiológicos sobre enfermedades como el VIH y Sida, en base a su necesidad para la salvaguarda de un interés general.
[2296] DE MIGUEL SÁNCHEZ, "Datos de carácter personal…", cit., 2010, p. 727; TRONCOSO REIGADA, "La comunicación de datos…", cit., 2010, p. 998.

El ordenamiento ofrece instrumentos suficientes para asumir esta interpretación[2297]. El argumento fundamental se encuentra en que la normativa sanitaria habilita en numerosas ocasiones cesiones de datos de carácter personal sin necesidad de recabar el consentimiento de los titulares, con el fin de proteger la salud pública. Primero, diferentes disposiciones que dirigen su regulación a la protección de dicho bien jurídico, en términos generales, justifican las cesiones de datos sin el consentimiento de su titular[2298]. Y, segundo, pueden encontrarse normas que reconocen supuestos en que los fines epidemiológicos justifican una cesión de datos sin necesidad de recabar el consentimiento. Las diferentes normas que regulan las redes de vigilancia epidemiológica, tanto a nivel estatal como autonómico, recogen la obligación de llevar a cabo cesiones por parte de los profesionales sanitarios de determinadas enfermedades consideradas de declaración obligatoria[2299]. En beneficio de la salud pública se prevén estas comunicaciones sin que sea necesario recabar el consentimiento de los titulares de los datos. En estas transmisiones se incluyen también datos referentes a la identidad de las personas afectadas[2300]. Es subrayable el hecho de que en casos excepcionales la propia jurisprudencia ha admitido que la salvaguarda de la salud pública exige del sacrifico del derecho a la autodeterminación informativa de determinados sujetos afectados por el VIH[2301].

[2297] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, pp. 46-47.

[2298] Artículo 5 Ley 25/1990, del Medicamento: *"Obligaciones de información entre las Administraciones Públicas.*
A efectos de salvaguardar las exigencias de salud y seguridad pública, las Administraciones Públicas están obligadas a comunicarse cuantos datos, actuaciones o informaciones se deriven del ejercicio de sus competencias y resulten necesarias para el correcto funcionamiento de esta ley".
Artículo 7.a) RD 711/2002, de 19 de julio, de Farmacovigilancia: *"Los médicos, farmacéuticos, enfermeros y demás profesionales sanitarios tienen la obligación de: notificar toda sospecha de reacción adversa de los que tengan conocimiento durante su práctica habitual y enviarla lo más rápidamente posible al órgano competente en materia de farmacovigilancia de la Comunidad Autónoma correspondiente (...)".*
Artículo 3 LO 3/1986, de Medidas Especiales en Materia de Salud Pública: *"Con el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible".*

[2299] Artículo 9 RD 2210/1995, 28 de diciembre, por el que se crea la Red Nacional de Vigilancia Epidemiológica: "*Las enfermedades objeto de declaración obligatoria se relacionan en el anexo I de este Real Decreto.*
La declaración obligatoria se refiere a los casos nuevos de estas enfermedades aparecidos durante la semana en curso y bajo sospecha clínica, y corresponde realizarla a los médicos en ejercicio, tanto del sector público como privado"; Artículo 12 Decreto 312/1996, 24 de diciembre de 1996, por el que se crea el Sistema de Vigilancia Epidemiológica en la Comunidad Autónoma del País Vasco: "*Declaración de enfermedades, alertas sanitarias y brotes epidémicos.*
1. Todos los médicos que ejercen en la Comunidad Autónoma del País Vasco así como los centros sanitarios ubicados en la misma están obligados a declarar al Sistema de Vigilancia Epidemiológica del País Vasco todos los supuestos incluidos en los apartados a) y b) del artículo 4 del presente Decreto, con la finalidad de desarrollar y evaluar las medidas de salud pública tendentes al control de las mismas en nuestro ámbito territorial."

[2300] Artículo 5 Orden de 27 de febrero de 2009, del Consejero de Sanidad, por la que se regula la declaración al Sistema de Información Microbiológica de la Comunidad Autónoma del País Vasco: "*Transferencia de datos.*
1. En la transferencia de datos al Sistema de Información Microbiológica deberán constar como mínimo las siguientes variables:
-Código de Identificación Corporativo (CIC).
-Nº Historia.
-Nombre.
-Apellidos.
-Fecha de nacimiento (...)"

[2301] STSJ de Galicia 21 de mayo del 2008, FJ 4.

Si bien en algún caso la doctrina se ha referido expresamente a la necesidad de que se respete el deber de secreto[2302], la excepción a consentir estas cesiones está plenamente justificada. La regulación prevista en las normas da pie a que la limitación al derecho a autorizar estas operaciones encuentre apoyo en diferentes argumentos.

En primer lugar, las referencias en la normativa "obligando" al profesional sanitario a llevar a cabo las citadas declaraciones entraría en la excepción al consentimiento en la cesión por previsión legal. Las leyes obligan a que se cree el flujo de información necesario para salvaguardar la salud pública. En segundo lugar, la justificación de la excepción podría tener otro fundamento, distinto al hecho de que las leyes prevean la necesidad de que las comunicaciones se produzcan. Concretamente, podría basarse también en razón de que estas cesiones se dan entre diferentes administraciones. Las normas hacen referencia constante a la importancia de las transmisiones entre órganos de diferentes administraciones. En la medida en que estas administraciones dirigen su actividad al cumplimiento de un mismo fin, la excepción a la necesidad de recabar el consentimiento del titular podría verse validada[2303]. En tercer lugar, la excepción tiene fundamento en el hecho de que la finalidad perseguida con las transmisiones de datos sanitarios no es otra que la salvaguarda de la salud pública.

Habiendo encontrado base jurídica suficiente para respaldar la posibilidad de exceptuar el derecho a consentir las cesiones de datos en esos supuestos, cabe preguntarse si estos argumentos servirían para admitir una limitación genérica a dicho derecho siempre que la salud pública esté en juego. De la lectura de la LOPD podría deducirse que todo estudio epidemiológico puede justificar la aplicación de la excepción, independientemente de las circunstancias de cada caso. Esta conclusión no puede ser seguida aquí. No hay que olvidar que la LBAP recoge una regulación opuesta a la prevista en la citada Ley. Se entiende que el principio de proporcionalidad ha de jugar, a falta de una previsión legal más concreta, un papel fundamental en la resolución de este enfrentamiento de intereses. Hay que traer aquí los argumentos que en el apartado dedicado a analizar el consentimiento justificaban la aplicación de la excepción.

Como punto de partida habrá de tenerse en cuenta que no todas las investigaciones tienen las mismas características. Hay que distinguir entre las que responden a un interés público y las que se hacen en beneficio de un interés particular. En el segundo supuesto será difícil justificar la excepción al consentimiento, mientras que si la investigación responde a un interés público de suficiente entidad, puede plantearse la aplicación de la excepción. No obstante, este límite no será de aplicación automática sino que se deberán tener en consideración determinados aspectos.

[2302] DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 118.
[2303] Artículo 21.1 LOPD.

De inicio, los datos médicos empleados con fines de investigación deberán ser anónimos[2304]. Sin embargo, cuando esta anonimización no sea posible o conveniente para el desarrollo adecuado de la investigación[2305], no siempre se deberá requerir el consentimiento de los titulares de los datos. En principio será necesario el consentimiento, pero cuando el recabar esta autorización conlleve un entorpecimiento del cumplimiento de la finalidad este requisito no será necesario[2306]. En las normas no se dice nada sobre quién deberá determinar si es posible emplear datos asociado a una persona identificada o identificable. Sin embargo, parece lógico pensar que podría contarse con las agencias de protección de datos o con algún comité médico para realizar dicho control previo[2307].

Cuando se tengan que manipular datos asociados con el fin señalado, en principio deberá respetarse el derecho a consentir de los titulares. Según la Recomendación del Consejo de Europa sobre la protección de datos médicos el derecho a consentir este tratamiento podrá limitarse cuando a criterio del organismo correspondiente creado para resolver estos conflictos la importancia de la investigación exigiera el tratamiento de la información de carácter personal sin dicho requisito[2308]. Este organismo, que podría ser una agencia de protección de datos, a la hora de excepcionar el consentimiento deberá atender a la importancia del interés que se protege, a

[2304] Artículo 16.2, LBAP; Artículo 12.1, R (97) 5. MUNAR BERNAT, "El Tratamiento...", cit., 1997, p. 132, apunta la posibilidad de que "incluso usando datos disociados, por la especificidad de la información empleada, (sea) relativamente sencillo ponerla en relación con el individuo de quien procede"; DE MIGUEL SÁNCHEZ, "Investigación y Protección…", cit., 2006, pp. 151-152.

[2305] RAMÍREZ NEILA, "Accesos legítimos…", cit., 2009, p. 296, apunta que no siempre cabe la anonimización cuando se emplean los datos con estos fines.

[2306] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 100.

[2307] HERRÁN ORTIZ, *El Derecho...,* cit., 2002, pp. 219-220.

[2308] Artículo 12 R(97) 5: *"Investigación científica.*

1.Siempre que sea posible, los datos médicos usados para fines de investigación científica deben ser anónimos. Los profesionales y organizaciones científicas y las autoridades públicas deben promover el desarrollo de técnicas y procedimientos para asegurar el anonimato.

2. Sin embargo, si tal anonimización hiciese imposible un proyecto científico de investigación, y el proyecto se va a realizar con fines legítimos, podría llevarse a cabo con datos personales a condición de que:

a)el titular de los datos haya dado su consentimiento informado para uno o más fines de investigación; o

b)otorguen el consentimiento el representante legal o la autoridad o persona u órgano previstos por la ley cuando el afectado sea una persona legalmente incapacitada e incapaz de una decisión libre, y la ley nacional no le permita actuar en su propia representación, siempre que este consentimiento se dé en el marco de un proyecto de investigación relacionado con la condición médica o la enfermedad del afectado; o

c) el órgano u órganos designados por la ley nacional hayan autorizado la revelación de los datos con el fin de llevar a cabo un proyecto de investigación médica relacionado con un interés público importante, pero sólo si:

i. el titular de los datos no se ha opuesto expresamente a la revelación; y

ii. a pesar de los esfuerzos razonables que se puedan adoptar, sería impracticable contactar con el titular de los datos para pedir su consentimiento; y

iii. el interés del proyecto de investigación justifica la autorización; o

d) la investigación científica está prevista por la ley y constituye una medida necesaria por razones de salud pública.

12. Bajo las previsiones complementarias que la ley nacional establezca, debe permitirse a los profesionales sanitarios habilitados para realizar su propia investigación médica el uso de los datos médicos que tienen en la medida en que el sujeto afectado haya sido informado de esta posibilidad y no se haya opuesto.

12. Respecto a cualquier investigación científica basada en datos personales, los problemas incidentales –incluidos aquellos de naturaleza ética y científica- que puedan surgir como consecuencia del respeto a las disposiciones de la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de datos

deben ser examinados también a la luz de otros instrumentos pertinentes

12. Los datos personales usados para investigación científica no pueden publicarse en forma que permita identificar a los titulares de los datos, salvo que éstos hayan dado su consentimiento a la publicación y ésta sea permitida por la ley nacional."

las medidas de seguridad que se van a adoptar para la salvaguarda de la autodeterminación informativa, a si existen o no formas alternativas para llevar a cabo la investigación, y a la necesidad real de interferir en el citado derecho fundamental de la persona[2309]. La posibilidad de que sea la agencia la que deba autorizar en determinados casos una investigación científica concreta que implica la manipulación de información de carácter personal, ya fue prevista en otros estados[2310].

Fundamentalmente habrá que tomar en cuenta dos elementos a la hora de determinar cuándo se puede aplicar la excepción al consentimiento. Primero hay que atender al bien jurídico que se protege con la investigación. Está asumida, hoy día, la gran importancia que esta operación tiene a efectos de salvaguardar la salud de los ciudadanos y la relevancia de los datos de carácter personal para llevarla adelante. La jurisprudencia ha determinado que "no existe avance científico fiable en ninguna enfermedad sin unas bases de datos fiables que muestren características del enfermo, costumbres, formas de vida, evolución ante tratamientos, años de investigación y medicamentos han tenido que arrinconarse por no haber tomado en consideración una determinada variable del paciente o de grupos de pacientes"[2311]. Esa misma jurisprudencia ha entendido que "el derecho a la protección de la salud, garantizado constitucionalmente, art. 43.1 CE, implica que se realicen todas las acciones que lo hagan efectivo"[2312]. Si bien la investigación, en general, constituye una actuación necesaria en la sociedad para la salvaguarda de la salud de los ciudadanos, tanto pública como individual, no se puede entender que todas las investigaciones incidan de la misma manera en la consecución de dicho fin. En esta línea, se ha subrayado en algún momento que "no todo proyecto intitulado <<científico>> amparará la cesión de datos (...) debiéndose analizar detenidamente y de forma individualizada a fin de determinar si efectivamente, a la vista del ente que desarrolla la investigación, el fin de la misma y la proporcionalidad de la intromisión o limitación del derecho

[2309] Punto 204, Memoria explicativa de la Recomendación R (97) 5 del Consejo de Europa: *"the authorisation, by the designated body, of communication of medical data for the purposes of a medical research project also depends on other factors implicit in the spirit of the recommendation in the present principle, or explicitly set out in other principles:*
a. the existence of alternative methods for the research envisaged;
b. the relevance of an important public interest of the aim of the research, for example in the field of epidemiology, of drug control or of the clinical evaluation of medicines;
c. the security measures envisaged to protect privacy;
d. the necessity of interfering in the privacy of the data subject".

[2310] Memoria AEPD, 1994: En relación al empleo de datos con el fin de llevar a cabo investigaciones de carácter médico, en el ámbito francés, pero teniendo en cuenta que se está hablando de 1994: "La nueva regulación refuerza las potestades de la CNIL en la medida en que, a diferencia del régimen general de la Ley de 1978, estos tratamientos requieren una autorización previa de la CNIL, a la cual se dota, a su vez, de un Comité consultivo que deberá juzgar en cada caso sobre la metodología de la investigación, la necesidad de utilizar datos personales y la pertinencia de estos para la finalidad de la investigación. (...)
En cuanto al régimen protector de los datos, los nuevos artículos 40.3, 40.4 y 40.5 contienen disposiciones que derogan o modulan disposiciones de la ley de 1978 y de otras leyes. El primero permite que los profesionales de la medicina cedan datos personales para que sean utilizados en tratamientos de investigación autorizados por la CNIL, pero para ello, los datos deberán ser codificados antes de ser cedidos. Esta norma de la codificación previa puede, sin embargo, ser dejada sin efecto en casos de tratamientos vinculados a estudios de vigilancia farmacéutica o de proyectos de cooperación nacional o internacional o <<si así lo exigiere una particularidad de la investigación>>. En todo caso, la exposición de los resultados de la investigación deberá ser despersonalizada, de tal manera que no sea posible identificar directa o indirectamente a los interesados".

[2311] STSJ de la Comunidad Valenciana, de 27 de noviembre 2002, FJ 3.

[2312] STS de 5 de junio de 1991, extraída de GIL-ROBLES y GIL DELGADO, "Los derechos...", cit., 1994, p. 89.

considerado que dicho estudio conlleve, puede efectivamente considerarse procedente". Se trataría pues, "de considerar las circunstancias concretas que concurrirían en cada supuesto sometido a la opinión de la Agencia de Protección de Datos, teniendo en cuenta, en especial, la normativa específica que pudiese resultar de aplicación al mismo"[2313]. La excepción deberá estar justificada caso por caso. Habrá que ver, por lo tanto, en qué medida la actuación que se pretende constituye una medida necesaria para proteger la salud de las personas.

Segundo, deberán tenerse en cuenta, a la hora de determinar la aplicabilidad de la excepción, las características particulares de los datos que se pretenden manipular en cada caso. En alguna ocasión la jurisprudencia ha señalado que, para interpretar la excepción al consentimiento que ahora se analiza, no se pueden hacer distinciones entre los diferentes datos de salud de una persona. Es decir, el mismo criterio se aplicará cuando se trate de información referente a un proceso gripal o lesión muscular que cuando concierna, por ejemplo, a una infección por el VIH[2314]. No tendría efectos jurídicos distintos el que sea uno u otro tipo de dato sanitario, pudiendo interpretarse que la excepción al consentimiento tendrá el mismo alcance en un caso que en el otro. Cierto es que de la letra de la Ley no se desprende distinción alguna entre los diferentes tipos de datos relativos a la salud de las personas. No obstante, esto no puede llevar a la conclusión planteada por el Tribunal.

Como se ha puesto de manifiesto reiteradamente, dentro de los datos relativos a la salud puede encontrarse información que afecta de forma más directa a la intimidad de las personas y cuyo conocimiento podría perjudicar de una manera especial[2315]. Se está hablando fundamentalmente de datos relativos a enfermedades mentales, prácticas abortivas o enfermedades contagiosas[2316]. La relevancia que en la sociedad actual se da a determinado tipo de información hace que este factor haya de ser tenido en cuenta al interpretar la excepción que se comenta. No será lo mismo limitar el derecho a consentir el tratamiento de un dato vinculado a un proceso gripal que el relacionado con una esquizofrenia.

Más allá de los estudios epidemiológicos, el criterio expuesto cabe emplearlo cuando lo que se quiere llevar a cabo son investigaciones de otra clase. Cuando se hace referencia a las investigaciones, no se está hablando de las investigaciones biomédicas o los ensayos clínicos en concreto. Las normas que regulan estas operaciones hacen referencia a la protección de datos, pero no disponen nada sobre la posibilidad concreta de emplear la información recabada de las investigaciones o los ensayos con fines de investigación. Indican, simplemente, que el uso de la información recogida, sea cual sea el fin, deberá sujetarse al consentimiento del titular[2317].

[2313] Memoria AEPD, 2002.
[2314] SAN 16 de enero de 2008 FJ 4.
[2315] Informe jurídico de la AEPD, 2 de abril de 2008, sobre las garantías de intimidad y protección de los datos de carácter personal de los usuarios del Sistema Nacional de Salud derivados a centros privados.
[2316] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), de 15 de febrero de 2007.
[2317] Artículo 3.6 RD 223/2004, 6 de febrero, por el que se regulan los Ensayos Clínicos con Medicamentos; Artículo 5 Ley 14/2007, 3 de julio de 2007, de Investigación Biomédica.

Interesa ahora la investigación, en términos genéricos, clínica o de carácter sanitario, que ha de sujetarse a la LBAP y LOPD[2318].

Se ha dicho que pueden encontrarse normas que exigen el consentimiento del titular de los datos para poder manipular la información con el objetivo de realizar investigaciones[2319]. Sin embargo, se acaban de dar argumentos para que la excepción al consentimiento tenga cabida también cuando se trata de perseguir estos fines. La cesión de datos sanitarios a determinados profesionales o la cesión entre diferentes equipos investigadores de la información resulta necesaria para realizar estos estudios. La finalidad no es otra que extraer información sobre determinadas enfermedades y posibles tratamientos. Sin duda, este objetivo cuenta con evidente trascendencia para la salvaguarda de la salud pública y también para la asistencia directa. La excepción al consentimiento a la hora de manipular información de carácter personal con la citada finalidad podrá encontrar justificación teniendo en cuenta los criterios que se han expuesto al analizar los estudios epidemiológicos.

Un instrumento fundamental dirigido a la protección de la salud pública lo constituye el CMBD, fijado en el sistema nacional de salud a partir de 1987[2320]. Esta herramienta no es otra cosa que un núcleo básico y mínimo de información sobre los diferentes episodios de hospitalización que han padecido las personas, que se incorpora a un registro[2321], constituyendo así una importante base de datos. La información se refiere, fundamentalmente, a datos de identificación del paciente, de identificación del episodio y datos clínicos. La base de datos que constituye este conjunto de datos se configura con información, tanto de contenido clínico como administrativo[2322], proveniente normalmente de los informes de alta o de las propias historias clínicas[2323]. Su relevancia reside en que se erige en fuente de información para determinar aspectos como la calidad de la gestión y de la asistencia, la necesidad de implantar nuevos sistemas de control de costes, criterios para llevar a cabo investigaciones clínicas y estudios epidemiológicos, etc[2324]. Es decir, aporta la suficiente información para fijar cuál es la situación de

[2318] VALCÁRCEL TEIJEIRO, "Protección de Datos…", cit., 2009, p. 97.

[2319] Artículo 16.3 LBAP; Artículo 8 Decreto 89/1999, 10 de junio, por el que se regula el Conjunto Mínimo Básico de Datos (CMBD) al alta hospitalaria y cirugía ambulatoria, en la Comunidad de Madrid: *"En los casos en los que se necesite utilizar datos de carácter personal para alguna investigación relacionada con este fichero se realizará con datos disociados, y si no pudieran ir disociados, se le pedirá el consentimiento expreso al ciudadano para poder utilizar sus datos con este fin*".

[2320] Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, nº 30, de 14 de diciembre de 1987, en http://www.msps.es

[2321] En el caso del País Vasco se trata del Registro de Altas Hospitalarias de Euskadi. Decreto 303/1992, 3 de noviembre, por la que se regula el Conjunta Mínimo Básico de Datos de Alta Hospitalaria y crea el Registro de Altas Hospitalarias de Euskadi.

[2322] Artículo 6 Orden 23 de noviembre de 1990, que regula el Informe Clínico y Conjunto Mínimo de Datos Básicos del Alta Hospitalaria de Cataluña: "*En el conjunto mínimo básico de datos de alta hospitalaria deben constar las siguientes variables: Código de centro o establecimiento; número de identificación del paciente; número de asistencia; fecha de nacimiento; sexo; residencia habitual; régimen económico de la asistencia prestada; fecha de admisión; circunstancias de admisión; fecha de alta; circunstancias de alta; código del centro de traslado, en su caso; diagnóstico principal; otros diagnósticos, en su caso; causas externas de la enfermedad, en su caso; procedimientos diagnósticos o terapéuticos; tiempo de gestación, en su caso; peso del recién nacido, en su caso; sexo del recién nacido, en su caso*".

[2323] PÉREZ GÓMEZ, "Protección de Datos…", cit., 2009, p. 40.

[2324] Exposición de Motivos Decreto 28/2007, 15 de marzo, que establece el Sistema de Información de Enfermedades Asistidas, regula el Conjunto Mínimo Básico de Datos (CMBD) al Alta Hospitalaria y Procedimientos Ambulatorios

un sistema sanitario y, además, puede constituir fuente de datos para llevar a cabo determinados estudios. La relevancia de esta fuente de información se sitúa, sobre todo, a nivel autonómico. Sin embargo, también constituye una fórmula para unificar criterios a la hora de transmitir información básica entre diferentes administraciones territoriales, como puede ser la cesión entre un sistema sanitario autonómico y el estatal. Es por esto que en todas las CCAA se ha de emplear el instrumento del CMBD.

Esta figura ha encontrado regulación en varias normas, sobre todo de carácter autonómico[2325]. Evidentemente, la creación y posterior empleo de estas bases de datos requiere de la transmisión de información sanitaria. Se puede plantear si las operaciones que se han de llevar a cabo para la creación de estas bases de datos exigen el consentimiento de los interesados. La doctrina parece haberse decantado por la aplicación de la excepción atendiendo a la relevancia de las finalidades[2326]. Esta interpretación tiene pleno sentido en la medida en que las normas citadas obligan a la realización de las operaciones necesarias para la creación de la base de datos[2327]. El uso que posteriormente se realizará de los datos contenidos en el registro deberá sujetarse a unas u otras normas dependiendo de la finalidad que se persiga y los demás parámetros que rodeen al tratamiento.

I.5.3.D.c. La cesión de datos de salud con finalidades relacionadas indirectamente con la asistencia sanitaria.

La excepción a la necesidad del consentimiento para llevar a cabo cesiones, justificada en la finalidad dirigida a la protección de la salud de las personas, puede tener su aplicación fuera de las actuaciones puramente asistenciales o médicas. Como se ha podido observar en el apartado dedicado al principio de finalidad, la actividad sanitaria va más allá de este concreto ámbito de actuación, englobando también funciones puramente administrativas. Se entendía entonces que

Especializados y crea el Registro del CMBD de la Comunidad de Castilla y León. MORENO VERNIS, "Documentación Clínica…", cit., 2002, pp. 21-24; PÉREZ GÓMEZ, "Protección de Datos…", cit., 2009, p. 40.

[2325] Orden 23 de noviembre de 1990, que regula el Informe Clínico y Conjunto Mínimo de Datos Básicos del Alta Hospitalaria de Cataluña; Decreto 303/1992, 3 de noviembre, por la que se regula el Conjunta Mínimo Básico de Datos de Alta Hospitalaria y crea el Registro de Altas Hospitalarias de Euskadi y orden de 3 de septiembre de 2010, del Consejero de Sanidad y Consumo, por la que se incorporan Nuevas Variables al Conjunto Mínimo Básico de Datos del Alta Hospitalaria; Decreto 89/1999, 10 de junio, por el que se regula el Conjunto Mínimo Básico de Datos (CMBD) al Alta Hospitalaria y Cirugía Ambulatoria, en la Comunidad de Madrid; Orden 4 de marzo de 2005, que regula el Conjunto Mínimo Basico de Datos (CMBD) al Alta Hospitalaria y Cirugía Mayor Ambulatoria y la Unidad Técnica de referencia CIE 9 MC de la Comunidad Autónoma de Extremadura; Decreto 28/2007, 15 de marzo, que establece el Sistema de Información de Enfermedades Asistidas, regula el Conjunto Mínimo Básico de Datos (CMBD) al alta hospitalaria y procedimientos ambulatorios especializados y crea el Registro del CMBD de la Comunidad de Castilla y León.

[2326] PÉREZ GÓMEZ, "Protección de Datos…", cit., 2009, p. 45.

[2327] Artículo 5 Orden 23 de noviembre de 1990, que regula el Informe Clínico y Conjunto Mínimo de Datos Básicos del Alta Hospitalaria de Cataluña: "*Todos los centros y establecimientos sanitarios asistenciales previstos en el artículo 1 quedan obligados a la elaboración del conjunto mínimo básico de datos de alta hospitalaria para todos los pacientes ingresados que hayan sido dados de alta y hayan producido, al menos, una estancia, el cual será enviado periódicamente al Department de Sanitat i Seguritat Social*". Artículo 2 Decreto 303/1992, 3 de noviembre, por la que se regula el Conjunta Mínimo Básico de Datos de Alta Hospitalaria y crea el Registro de Altas Hospitalarias de Euskadi: "*Todos los Centros Hospitalarios, tanto públicos como privados, radicados en la Comunidad Autónoma del País Vasco, quedan obligados a garantizar la elaboración y la posterior comunicación del Conjunto Mínimo Básico de Datos del Alta Hospitalaria al Registro que a tal efecto se crea en el Departamento de Sanidad del Gobierno Vasco*".

estas acciones constituían una pieza más en el desarrollo de la actividad sanitaria. Es por ello por lo que se puede plantear si las cesiones que se dan en el ejercicio de estas funciones se pueden llevar a cabo sin el consentimiento del titular de los datos, pero respetando en todo caso los principios que determinan la calidad de los datos, es decir, teniendo acceso solamente a la información que se estime necesaria para el ejercicio de sus funciones[2328].

A) En primer lugar, existen finalidades relacionadas con el buen funcionamiento del sistema sanitario pero que no se refieren a la asistencia médica directa. Un ejemplo de lo dicho lo constituyen los trabajos de inspección del sistema sanitario, que en ocasiones llevan a cabo las propias administraciones y a veces empresas externas[2329]. Lo mismo ocurre con el control, desde un punto de vista económico, de la actividad que se desarrolla en un centro sanitario. En estos casos la finalidad inmediata no es la salvaguarda de la salud de las personas. Sin embargo, la relevancia de estas operaciones está fuera de duda. El correcto funcionamiento de la Administración sanitaria requiere que se controlen diferentes aspectos de la misma: gestión económica, ejercicio de las distintas profesiones, entre otras. El ejercicio de estas funciones exige en ocasiones del acceso a las historias clínicas, para conocer las características concretas de las actuaciones llevadas a cabo en un momento determinado. Las normas crean órganos que dirigen su actividad a realizar estas labores fiscalizadoras. Muchas veces, al centralizarse estos órganos en el Estado, estas funciones exigen que se lleven a cabo diferentes transmisiones de información desde las CCAA[2330]. Para estos casos parece asumirse la posibilidad de ceder datos sanitarios, incluso sin el consentimiento del titular[2331].

En la normativa sanitaria interna pueden encontrarse referencias a estos supuestos. En el ámbito autonómico alguna norma ha reconocido la posibilidad de que el personal sanitario acreditado acceda a la información sanitaria con los fines citados, si bien limitando dicho acceso a datos anonimizados. En el supuesto de que no lo estén, será necesario el consentimiento del titular para que el acceso pueda producirse[2332]. En un sentido distinto, la LBAP, al igual que otras

[2328] MARTÍ MONTESINOS, PIDEVALL BORRELL, "Accesos a la Historia…", cit., 2004, p. 108.

[2329] CASTELLANO ARROYO, "Problemática de la historia...", 1997, cit., p. 63, afirma que no es "adecuado a la legislación vigente (en referencia al artículo 61 de la LGS) que la inspección de historias clínicas pueda ser encargada a agencias o empresas expertas en controles de calidad o similares".

[2330] Artículo 79 Ley 16/2003, 28 de mayo, de Cohesión y Calidad del Sistema Nacional de Salud: "*Coordinación y cooperación de la inspección en el Sistema Nacional de Salud.*
La Alta Inspección del Estado establecerá mecanismos de coordinación y cooperación con los servicios de inspección de las comunidades autónomas, en especial en lo referente a la coordinación de las actuaciones dirigidas a impedir o perseguir todas las formas de fraude, abuso, corrupción o desviación de las prestaciones o servicios sanitarios con cargo al sector público, cuando razones de interés general así lo aconsejen.
Para ello, la Alta Inspección desarrollará las siguientes actividades:
a) La creación y mantenimiento de una base de datos compartida con los servicios de inspección del Sistema Nacional de Salud.
b) El desarrollo de la colaboración entre los diferentes servicios de inspección en el Sistema Nacional de Salud en programas de actuación conjunta en materia de control de evaluación de servicios y prestaciones.
c) El seguimiento, desde los ámbitos sanitarios, de la lucha contra el fraude en el Sistema Nacional de Salud, tanto en materia de la incapacidad temporal, como de los programas que se puedan promover en relación con áreas identificadas como susceptibles de generar bolsas de fraude en prestaciones o supongan desviaciones de marcada incidencia económica".

[2331] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, pp. 47-48 y. 83.

[2332] Artículo 12 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el Uso y Acceso a la Historia Hlínica Electrónica: *"El sistema IANUS permitirá el acceso a la información contenida en la historia clínica electrónica al*

normas autonómicas, recoge una regulación diferente al disponer que los profesionales acreditados "tienen acceso" a las historias clínicas para cumplir sus funciones, sin hacer referencia a que los datos deban estar anonimizados o no[2333]. En la medida en que se les reconoce la posibilidad de acceder a estos documentos, no parece que el consentimiento del titular de los datos sea necesario. Desde instancias supranacionales pueden encontrarse pronunciamientos acordes a este último criterio. Se ha previsto que en determinados casos es necesaria la cesión de datos sanitarios con el fin de cumplir objetivos no asistenciales, pero sí vinculados directamente a la prestación de esos servicios[2334]. De la misma manera, de la LOPD se deduce que no se requiere el consentimiento del titular para manipular datos cuando el fin es la "gestión de servicios sanitarios"[2335]. No parece difícil vincular las actividades que en este apartado se comentan a labores de gestión. La jurisprudencia ha admitido también la importancia de facilitar la realización de estas inspecciones, excluyendo la necesidad del consentimiento del titular de los datos[2336]. Más allá de la contradicción que se pueda generar entre lo que disponen determinadas normas, no parece haber problema para admitir la posibilidad de exceptuar el consentimiento con los fines que se han citado[2337].

La justificación de esta interpretación podría basarse en diferentes argumentos. La existencia de una previsión legal justificaría por sí sola esta comunicación sin el consentimiento del

---

personal debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación sanitaria, en la medida en que lo precise para el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, del respeto de los derechos del/de la paciente o de cualquier otro deber del centro en relación con los/as pacientes y usuarios/as o la propia Administración sanitaria. El acceso mencionado tendrá el alcance de la labor encomendada por la autoridad competente, y respetará el derecho a la intimidad personal y familiar de los/as pacientes o usuarios/as.

El acceso a la información contenida en la historia clínica electrónica con fines de evaluación, acreditación y planificación sanitaria obliga a preservar los datos de identificación personal del/de la paciente o usuario/a, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, excepto que el/la propio/a paciente o usuario/a diese su consentimiento para no separarlos".

[2333] Artículo 16.5 LBAP: "*El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos de los pacientes o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración Pública";* Artículo 33, Ley 8/1997, 26 de junio de 1997, de Ordenación Sanitaria de Euskadi*: "El personal al servicio de las Administraciones públicas que desarrolle las funciones de inspección debidamente acreditado podrá realizar cuantas actuaciones se requieran para el cumplimiento de la función inspectora, en especial:*

a) Entrar libremente en cualquier dependencia del centro o establecimiento sujeto a esta ley, sin necesidad de previa notificación.

b) Proceder a las pruebas, investigaciones o exámenes necesarios para comprobar el cumplimiento de lo previsto en esta Ley y en las normas que se dicten para su desarrollo".

[2334] Punto 143, párrafo 2, Memoria Explicativa Recomendación R (97) 5 del Consejo de Europa: "*There are however certain circumstances under which relevant medical data must be disclosed to other persons or bodies which, while not in charge of the medical treatment of the data subject, act otherwise in his/her direct interest (for example social security services), or are in charge of medical research (...)*".

[2335] Artículo 7.6 LOPD.

[2336] AAP Segovia, nº 95/2000, Sección única, justifica la potestad del INSALUD para llevar a cabo acciones de inspección, para lo cual es necesario que tenga la posibilidad de acceder a las historias clínicas: "las tareas encomendadas legislativamente al Insalud, de evaluación y control, resultarían baldías si no pudiera acceder a esta historia (...) además, resulta autorizado el acceso a efectos de inspección".

[2337] Resolución de la APDCM, 18 de septiembre de 2009, "La cesión de datos no requiere consentimiento cuando está amparada por Ley", en la que se afirma que la cesión con fines de inspección no requiere del consentimiento al estar habilitada por la LBAP.

titular[2338]. En este sentido la LBAP constituiría base suficiente para considerar que dicha previsión existe de manera genérica habilitando las transmisiones de la información[2339]. También podría alegarse, que el hecho de que la finalidad perseguida sea de indudable interés general justifica la excepción al consentimiento. Controlar que la actividad de los centros sanitarios es adecuada o correcta repercute, en última instancia, en la obtención de un buen servicio sanitario, lo cual de forma mediata beneficia a los ciudadanos en lo que respecta a la protección de su salud. Este fin puede constituir argumento suficiente, para justificar las cesiones a los funcionarios que han de ejercer el control del que se habla, siempre y cuando se respeten los principios que determinan la calidad de los datos y el derecho a ser informado[2340].

B) En segundo lugar, otro supuesto de cesión de datos vinculada a actividades que indirectamente tienen que ver con la asistencia sanitaria puede reconocerse en determinadas comunicaciones a favor de los colegios profesionales. Se está hablando de las cesiones de datos dirigidas a controlar la actividad de los profesionales sanitarios. En una actividad tan compleja como la sanitaria es importante la función de los colegios profesionales. Ya se han comentado más arriba las circunstancias que rodean a las comunicaciones de datos a estos entes, fundamentalmente las particularidades que derivan del hecho de que desarrollan actividades tanto de interés público como privado. Se señalaban las diferentes funciones que desarrollan estas instituciones colegiales, destacando como actividades que pueden tener una mayor incidencia en el control de la actividad sanitaria, las dirigidas a la adopción de las medidas necesarias para evitar el intrusismo profesional y al ejercicio de potestades disciplinarias[2341]. Sin duda el ejercicio de estas funciones requiere el acceso a determinados datos, la mayoría de veces a los datos referentes a la persona y la actividad del profesional sanitario[2342]. La cesión de esta información a los colegios profesionales podría llevarse a cabo sin el consentimiento del titular. La justificación de esta excepción se podría situar en que la finalidad última consiste en el buen funcionamiento del sistema sanitario.

C) En tercer lugar, otra actividad de especial relevancia, vinculada con la sanidad pero que no se corresponde con la asistencia sanitaria directa, es el de la docencia. El ordenamiento ha subrayado la importancia de esta actividad, obligando a las administraciones a tomar las medidas oportunas para que la formación de futuros profesionales de la sanidad sea posible[2343]. Las

[2338] Apartado 3.3,e) Recomendación 2/2004, de 30 de julio, de la Agencia de Protección de Datos de la Comunidad de Madrid, sobre Custodia, archivo y seguridad de los datos de carácter personal de las historias clínicas no informatizadas.
[2339] Artículo 16.5 LBAP.
[2340] STS 13 de mayo de 2009, FJ 8, pone de manifiesto la necesidad de que los órganos administrativos limiten sus accesos a determinados datos de contenido no clínico. Dictamen AVPD CN10-004, 8 de marzo de 2010, en el que se justifica el acceso de personal administrativo a determinada información con fines de carácter administrativo, si bien limita esta facultad de acceso a los datos necesarios para realizar esas funciones, negando la posibilidad de acceso a las historias clínicas.
[2341] Artículo 5 Ley 2/1974, de 13 de febrero de 1974, sobre Colegios Profesionales: "*Corresponde a los Colegios Profesionales el ejercicio de las siguientes funciones, en su ámbito territorial: i. Ordenar en el ámbito de su competencia la actividad profesional de los colegiados, velando por la ética y dignidad profesional y por el respeto debido a los derechos d e los particulares y ejercer la facultad disciplinaria en el orden profesional y colegial; (…) l. Adoptar las medidas conducentes a evitar el intrusismo profesional*".
[2342] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 236.
[2343] Artículo 104 LGS: "*1. Toda la estructura asistencial del sistema sanitario debe estar en disposición de ser utilizada para la docencia pregraduada, postgraduada y continuada de los profesionales.*

personas que se están formando deberán tener acceso a las herramientas o instrumentos de que disponen los centros sanitarios. Entre estas herramientas se encuentra la historia clínica de pacientes. La cesión de datos relativos a la salud de una persona al ámbito docente, para preparar futuros profesionales, podría verse como una función vinculada de manera mediata con la mejora del servicio sanitario.

¿Podría justificar esta circunstancia la aplicación de la excepción al consentimiento? No parece que los argumentos citados puedan superar el juicio de proporcionalidad[2344]. No es aceptable que para llevar a cabo la función docente sea necesario que los alumnos tengan acceso a las historias clínicas completas. Así, dispone la LBAP que en estos supuestos la cesión deberá realizarse en todo caso tras un proceso previo de disociación[2345]. No es necesario que en la documentación a la que han de acceder los alumnos se dé la relación entre la identidad de los pacientes y los datos relativos a su salud. De inicio, por lo tanto, los principios que determinan la calidad de los datos llevan a que sea exigible la disociación de la información que se transmita a los centros. El único caso en que se podría justificar el acceso de estos alumnos a los datos sanitarios de un sujeto es el que se da cuando están realizando prácticas y su actividad se dirige a salvaguardar la salud del titular de los datos. La finalidad, en este caso, sería la asistencia directa por lo que el juicio de proporcionalidad resultaría superado. En todo caso, sobra decir, los profesores y alumnos que tienen acceso a esa información deberán de guardar y respetar el secreto profesional[2346].

En todos los supuestos que se acaban de analizar las cesiones se dirigen al cumplimiento de fines que no se corresponden con la protección inmediata de la salud, si bien la finalidad se vincula, aunque de forma mediata, con el buen funcionamiento del sistema sanitario. Indudablemente, estas cesiones han de llevarse a cabo con todas las garantías. Será fundamental, en este sentido, respetar el deber de guardar secreto por parte de quien tenga acceso a la información sanitaria[2347] y asegurar que los accesos a los ficheros por parte de estos sujetos queden registrados, de tal forma que dichas actuaciones sean controlables. De la misma forma, será necesario ponderar si para llevar a cabo el fin concreto que se pretende es imprescindible la asociación entre los datos y la identidad de los usuarios. Por ejemplo, cuando el

2. Para conseguir una mayor adecuación en la formación de los recursos humanos necesarios para el funcionamiento del sistema sanitario se establecerá la colaboración permanente entre el departamento de Sanidad y los Departamentos que correspondan, en particular el de Educación y Cultura, con objeto de velar porque toda la formación que reciban los profesionales de la salud pueda estar integrada en las estructuras de servicios del sistema sanitario.

3. Las Administraciones públicas competentes en Educación y Sanidad establecerán el régimen de conciertos entre las Universidades y las instituciones sanitarias en las que se debe impartir enseñanza universitaria, a efectos de garantizar la docencia práctica de la medicina"; Artículo 12 y siguientes, Ley 44/2003, de 21 de noviembre de 2003, de ordenación de las profesiones sanitarias.

[2344] VERDÚ PASCUAL, *Secreto Profesional…,* cit., 2005, p. 75.

[2345] Artículo 16.3 LBAP.

[2346] BAZÁN ÁLVAREZ, "El consentimiento…", cit., 2004, p. 217.

[2347] Punto 144 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: "*such communication may only be made to persons bound by confidentiality, unless the domestic law provides for other safeguards. The rules of confidentiality are medical secrecy, for the medical sector or comparable rules for other sectors*"; MARTÍ MONTESINOS, PIDEVALL BORRELL, "Accesos a la historia...", cit., 2004, p. 109: en relación al acceso de personal con fines de inspección: "Es destacable que la autorización recae exclusivamente en personal sanitario**,** el que a su vez tiene un específico deber de secreto".

tratamiento de la información se realiza con objetivos estadísticos, fin de especial importancia a la hora de valorar diferentes aspectos de un sistema sanitario determinado, resulta evidente que bastará con hacerse con datos disociados[2348].

I.5.4. La cesión de datos sanitarios fuera del ámbito médico.

En todos los supuestos analizados hasta ahora los datos no salen del ámbito sanitario. Este sector, como se ha venido subrayando, está rigurosamente afectado por la obligación de secreto médico de tal modo que la cesión se produce en un ámbito de mayor seguridad. En el apartado que sigue se analizarán los casos en que los datos salen de este entorno.

I.5.4.A. El riesgo de que los datos de salud salgan del ámbito sanitario.

Las cesiones dentro del ámbito sanitario tienen, como se ha visto, justificación en diferentes supuestos. Han de plantearse en este momento otros espacios de la realidad a los que esta información puede comunicarse. Se está haciendo referencia a las transmisiones fuera del citado sector. La doctrina ha manifestado que estas cesiones constituyen uno de los principales problemas en el tratamiento de los datos de salud[2349].

El daño que puede generar un uso irregular de los datos de salud de las personas lleva a que exista una honda preocupación porque este tipo de información pueda salir del ámbito en que inicialmente ha de manipularse. El Consejo de Europa, a la hora de regular las bases de datos médicos, desde siempre ha puesto el acento en el riesgo que supone que esas bases de datos sean conocidas por sujetos externos al ámbito sanitario. La Recomendación que regulaba los Bancos de Datos Médicos de 1981 establecía que ni el contenido ni la mera existencia de las historias clínicas pueden ser comunicados a sujetos que se encuentren fuera del ámbito de la asistencia e investigación sanitaria, a no ser que así lo autorice el titular de los datos con su consentimiento expreso e informado o lo habiliten las normas reguladoras del secreto profesional[2350]. La actual Recomendación sobre la Protección de los Datos Médicos parte de la base de que estos datos, teniendo carácter sensible, no pueden ser comunicados fuera del ámbito sanitario en el que fueron recogidos, a no ser que estén disociados[2351]. En el ámbito estatal esta situación se refleja expresamente en el Cogido de Ética y Deontología Médica, en el que se subraya la necesidad de que las bases de datos sanitarias no se conecten con redes informáticas no médicas[2352]. También en algunas normas que regulan aspectos concretos del

[2348] SAN 27 de febrero de 2008, FFJJ 2-3, hace referencia a este supuesto.

[2349] LEGALIA, *La Protección...*, cit., 2002, p. 103, apunta que uno de los "problemas más importantes que se producen en relación con los datos de salud es el de la multiplicidad de usos que pueden darse de los mismos y, en consecuencia, de sus potenciales usuarios".

[2350] Artículo 5.4 Recomendación nº (81) 1, 23 de enero de 1981, que en su versión original en ingles señala: *"Without the data subject's express and informed consent, the existence and content of his medical record may nor be communicated to persons or bodies outside the fields of medical care, public health or medical research, unless such a communication is permitted by the rules on medical professional secrecy"*.

[2351] Punto 143 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: "*It is obvious that medical data, one of the categories of sensitive data for which the convention requires special protection, should not be communicated outside the medical context in which they were collected, unless they are made anonymous (in which case the data no longer fall under the definition of personal data)*".

[2352] Artículo, 17.4 Código de Ética y Deontología Médica: *"los bancos de datos médicos no pueden ser conectados a una red informática no médica"*. Se sigue, en este sentido, el criterio establecido por la Guía de Ética Médica europea

tratamiento de datos sanitarios se intuye la preocupación de que esta información salga del ámbito estrictamente médico. En la normativa laboral, por ejemplo, se parte de la premisa de que sólo el personal médico y las autoridades sanitarias pueden tener acceso a los datos de salud[2353].

La jurisprudencia, por su parte, también ha subrayado la importancia de que estos datos se mantengan, en la medida de lo posible, en el ámbito estrictamente sanitario[2354]. El TEDH ha sancionado, por ejemplo, el que un tribunal haya publicado en una sentencia la condición de seropositivo de un sujeto, identificándolo con su nombre y apellidos completos. Subraya expresamente la relevancia de que este tipo de información no se difunda fuera del entorno sanitario[2355].

En cualquier caso, a pesar de que de inicio el ordenamiento muestre cierta cautela a la hora de admitir cesiones de datos relativos a la salud de las personas, que llevan a este tipo de información fuera del ámbito sanitario, las normas reconocen diferentes supuestos en que estas transmisiones tienen plena justificación.

I.5.4.B. La cesión de datos sanitarios al Defensor del Pueblo.

Uno de los casos más conocidos en que los datos sanitarios se comunican fuera del ámbito médico lo constituye la cesión a Jueces y Tribunales, que más adelante se analizará. Cabe plantearse ahora si, al igual que en este caso, puede transmitirse la información a otros órganos que dirigen su actividad a la defensa de los derechos fundamentales, sin necesidad de obtener el

---

de 6 de enero de 1987 que en su artículo 8º dispone que "*los bancos de datos médicos no podrán estar conectados con otros bancos de datos"*.

[2353] Artículo 22.4 la Ley 31/1995, de 8 de noviembre de 1995, de Prevención de Riesgos Laborales: *"El acceso a la información médica de carácter personal se limitará al personal médico y a las autoridades sanitarias que lleven a cabo la vigilancia de la salud de los trabajadores, sin que pueda facilitarse al empresario o a otras personas sin consentimiento expreso del trabajador.*
No obstante lo anterior, el empresario y las personas u órganos con responsabilidad en materia de prevención serán informados de las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo o con la necesidad de introducir o mejorar las medidas de protección y prevención, a fin de que puedan desarrollar correctamente sus funciones en materia preventiva". STS 20 de octubre de 2009, FJ 5, subraya que "la regla general es la confidencialidad de toda la información obtenida por las mutuas en aplicación de la Ley de Prevención de Riesgos Laborales y, por consiguiente, que la posibilidad de comunicar al empresario "las conclusiones que se deriven de los reconocimientos efectuados en relación con la aptitud del trabajador para el desempeño del puesto de trabajo" constituye una excepción. Y las excepciones, como es bien sabido, han de ser interpretadas restrictivamente. En este supuesto, además, ello resulta reforzado por una consideración teleológica innegable: si lo que debe protegerse ante todo es la confidencialidad de la información sanitaria relativa a los trabajadores, no tiene sentido afirmar que cabe comunicar a los empresarios cualquier dato que exceda de la mera "conclusión" sobre la idoneidad del trabajador para el puesto de trabajo". TASCÓN LÓPEZ, *El Tratamiento por la Empresa…,* cit., 2005, pp. 98-99; FERNÁNDEZ-COSTALES MUÑIZ, "La Confindecialidad de los Datos…", cit., 2008, p. 127; RODRÍGUEZ ESCANCIANO, Susana, *El derecho a la protección…,* cit., 2009, pp. 53-57.

[2354] SAN 9 de julio 2008, FJ 4.

[2355] STEDH 6 de octubre de 2009, C. C. v. España, FFJJ 26-41.

consentimiento del titular de los datos. Un ejemplo claro al respecto de lo que se acaba de señalar lo constituye la cesión de datos sanitarios a favor del Defensor del Pueblo[2356].

La LOPD recoge expresamente, para las cesiones de los datos denominados comunes, la excepción al derecho a consentir las comunicaciones cuando la transmisión tenga por destinatario, entre otros, al Defensor del Pueblo, siempre y cuando esta operación se lleve a cabo en el ámbito de sus funciones[2357]. Esta regulación se reconoce en la Ley cuando hace referencia al régimen jurídico de las cesiones. Es decir, concierne a los datos comunes, sin que se haga alusión a su aplicabilidad a los datos que son objeto de una especial protección, caso de los de salud. Esta circunstancia plantea la duda de si esta regulación, la excepción, es directamente aplicable desde la LOPD a los datos sanitarios. Es necesario encontrar apoyo en otros argumentos más sólidos para justificar la aplicación de esta excepción al consentimiento.

La base del límite al derecho a consentir puede encontrarse en este caso en las leyes. La LBAP no dice nada al respecto. Sin embargo, tanto en el ordenamiento estatal como autonómico pueden encontrarse normas que reconocen la necesidad de que el Defensor del Pueblo acceda a la información necesaria para poder llevar a cabo sus funciones. Así lo hacen las leyes que regulan el funcionamiento de esta figura[2358]. Señalan las leyes que todos los organismos sujetos al control de esta institución estarán obligados a colaborar con la misma[2359]. Es más, en esta regulación se reconoce la posibilidad de que el Defensor acceda incluso a información clasificada como reservada o secreta[2360].

[2356] Artículo 54 CE: "*Una ley orgánica regulará la institución del Defensor del Pueblo, como alto comisionado de las Cortes Generales, designado por éstas para la defensa de los derechos comprendidos en este Título, a cuyo efecto podrá supervisar la actividad de la Administración, dando cuenta a las Cortes Generales*".

[2357] Artículo 11.2 LOPD: "*El consentimiento exigido en el apartado anterior no será preciso:*
d) cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo (...) en el ejercicio de las funciones que tiene atribuidas (...)"; Artículo 10.4.b) RDLOPD.

[2358] Artículo 19.2 LO 3/1981, de 6 de abril de 1981, del Defensor del Pueblo: "*En la fase de compilación e investigación de una queja o en un expediente iniciado de oficio, el Defensor del Pueblo, su adjunto o la persona en quien el delegue, podrán personarse en cualquier centro de la Administración pública, dependientes de la misma o afectos a un servicio público, para comprobar cuantos datos fueren menester, hacer las entrevistas personales pertinentes o proceder al estudio de los expedientes y documentación necesaria*"; Artículo 12, Ley 3/1985, 27 de febrero de 1985, por la que se Crea y Regula la Institución del Ararteko: "*Para el correcto ejercicio de las facultades y competencias el Ararteko actuará con medios informales y expeditivos. A tal efecto podrá: a) Efectuar visitas de inspección a cualquier servicio o dependencia de los organismos y entidades a que se refiere el artículo 9.1, examinando documentos, oyendo a órganos, funcionarios o trabajadores y solicitando las informaciones que estime convenientes. b) Proceder a cuantas investigaciones estime convenientes, siempre que no colisionen con los derechos o intereses legítimos de los ciudadanos y de las entidades sujetas a control (...)*".

[2359] Artículo 19 LO 3/1981, de 6 de abril de 1981, del Defensor del Pueblo: "*1. Todos los poderes públicos están obligados a auxiliar, con carácter preferente y urgente al Defensor del Pueblo en sus investigaciones e inspecciones*"; Artículo 23 Ley 3/1985, de 27 de febrero de 1985, por la que se Crea y Regula la Institución del Ararteko: "*Los órganos de las Entidades a que se refiere el artículo 9.1 tienen el deber de aportar, con carácter preferente y urgente, cuantos datos documentos, informes o aclaraciones les sean solicitados*". DE PALACIO VALLE-LERSUNDI, "Artículo 19…", cit., 2002, p. 491.

[2360] Artículo 22 LO 3/1981, de 6 de abril de 1981, del Defensor del Pueblo: "*1. El Defensor del Pueblo podrá solicitar a los poderes públicos todos los documentos que considere necesarios para el desarrollo de su función, incluidos aquellos clasificados con el carácter de secretos de acuerdo con la Ley. En este último supuesto la no remisión de dichos documentos deberá ser acordada por el Consejo de Ministros y se acompañará una certificación acreditativa del acuerdo denegatorio (...)*"; Artículo 15 Ley 3/1985, de 27 de febrero de 1985, por la que se Crea y Regula la Institución del Ararteko: "*1. La calificación de un documento como secreto oficial, de acuerdo con la legislación vigente, no impedirá su conocimiento por el Ararteko.*

Teniendo en cuenta las previsiones legales parece clara la facultad del Defensor del Pueblo de acceder a la información sanitaria con el fin de controlar de oficio la actuación de los centros, o con el objetivo de atender a las quejas de particulares que hayan podido ver sus derechos fundamentales lesionados por la actuación de la Administración sanitaria[2361]. La "obligación" que establecen las leyes de colaborar con esta institución constituye base suficiente para entender que la excepción al consentimiento es aplicable. Además, parece que si se reconoce la posibilidad de que este órgano acceda a información considerada secreta o reservada, debe admitirse la posibilidad de que se cedan a su favor otros datos de menor relevancia, como podrían ser los datos de salud de determinados sujetos.

Podría pensarse que la conclusión a la que se acaba de llegar limita en exceso el derecho a la autodeterminación informativa de los pacientes, si se tiene en cuenta que no se trata de un órgano judicial. No obstante, la relevancia del Defensor del Pueblo ha sido suficientemente contrastada tanto por las leyes como por la jurisprudencia y la doctrina. La CE crea esta figura como órgano que dirige su actividad a la protección de los derechos fundamentales[2362]. Su importancia se deja entrever en el texto de la Constitución al disponer que este órgano cuenta con la facultad de interponer ante el TC los recursos de inconstitucionalidad y de amparo[2363]. La doctrina, por su parte, ha subrayado en innumerables ocasiones la importancia de la función de control que ejerce sobre los poderes públicos[2364]. Así lo ha hecho también la jurisprudencia[2365].

A pesar de tratarse de una facultad de control de alguna manera limitada, pues el Defensor del Pueblo carece de potestad sancionadora ejecutable sobre las instituciones que hayan actuado de forma irregular[2366], es indudable que la capacidad de persuasión de este órgano es significativa. Por un lado, a través de sus informes pone de manifiesto la deficiente actuación de los poderes públicos, a los que compele a reorientar su actividad[2367]. Por otro, mediante su actuación "como impulsor de la actividad jurisdiccional"[2368] o impulsor también de la actuación de control llevada a cabo por órganos constitucionales, como los distintos parlamentos[2369], tiene

---

2. No obstante lo prevenido en el apartado anterior, el Gobierno, mediante acuerdo expreso al respecto, podrá denegar el acceso del Ararteko a dicha documentación (...)".VARELA SUANCES-CARPEGNA, "La naturaleza jurídica…", cit., 1983, p.70; LUNA ABELLA, "Artículo 22…", cit., 2002, p. 573.

[2361] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 235.

[2362] Artículo 54 CE.

[2363] Artículo 162.1 CE.

[2364] VARELA SUANCES-CARPEGNA, "La naturaleza jurídica…", cit., 1983, p. 67; CORCHETE MARTÍN, *El Defensor del Pueblo…*, cit., 2001, p. 92; ROVIRA VIÑAS, "Introducción…", cit., 2002, pp. 32-33.

[2365] STC 15 de noviembre del 2000, FJ 2.

[2366] CARBALLO ARMAS, *El Defensor del Pueblo…,* cit., 2003, p. 154.

[2367] Artículo 32 LO 3/1981, 6 de abril de 1981, del Defensor del Pueblo: "*1. El Defensor del Pueblo dará cuenta anualmente a las Cortes Generales de la gestión realizada en un informe que presentará ante las mismas cuando se hallen reunidas en periodo ordinario de sesiones.*

2. Cuando la gravedad o urgencia de los hechos lo aconsejen podrá presentar un informe extraordinario que dirigirá a las Diputaciones Permanentes de las Cámaras si estas no se encontraran reunidas".

[2368] CARBALLO ARMAS, *El Defensor del Pueblo…,* cit., 2003, p. 156.

[2369] Artículo 23 LO 3/1981, 6 de abril de 1981, del Defensor del Pueblo: "*Cuando las actuaciones practicadas revelen que la queja ha sido originada presumiblemente por el abuso, arbitrariedad, discriminación, error, negligencia u omisión de un funcionario, el Defensor del Pueblo podrá dirigirse al afectado haciéndole constar su criterio al respecto. Con la misma fecha dar traslado de dicho escrito al superior jerárquico formulando las sugerencias que considere oportunas*". Artículo 25 LO 3/1981, 6 de abril de 1981, del Defensor del Pueblo : "*Cuando el Defensor del Pueblo, en razón del ejercicio de las funciones propias de su cargo, tenga conocimiento de una conducta o hechos*

capacidad para promover acciones directas sobre determinados organismos que, según su criterio, han actuado de manera no acorde a la Ley. Por último, mediante la publicación de sus informes, el Defensor del Pueblo cuenta con una significativa influencia sobre la conformación de la opinión pública, que no hay que obviar. Es conocida la importancia que los medios otorgan a dichos documentos como fuentes de información[2370]. La relevancia de esta función de control bien merece, se entiende aquí, que el acceso del Defensor del Pueblo a los datos sanitarios contenidos en la Administración sanitaria se pueda llevar a cabo sin la necesidad del consentimiento del titular. Es evidente que en última instancia esta actuación repercutirá en el mejor funcionamiento de esta Administración.

Hay que tener en cuenta además que la normativa que regula el funcionamiento del Defensor del Pueblo establece garantías suficientes, dirigidas a proteger el derecho a la autodeterminación informativa y la intimidad de las personas afectadas en las investigaciones que lleva a cabo. Se obliga a esta institución a guardar o respetar el deber de secreto sobre los datos que conoce fruto de su trabajo[2371] y, en concreto, en relación a los informes a presentar a las Cortes Generales, se prohíbe que en los mismos se publique la identidad de los sujetos interesados en los procedimientos investigadores[2372]. La previsión de estas garantías hace que el acceso de este órgano a los datos de carácter personal pueda darse afectando en la menor medida posible a los derechos de intimidad y de autodeterminación informativa.

En relación a un supuesto semejante al expuesto en este punto, algún informe jurídico de la AEPD ha reconocido la posibilidad de transmitir al Defensor Universitario información referente a los diferentes agentes que actúan en el ámbito universitario, siempre y cuando la cesión se dirija al cumplimiento de sus funciones en defensa de los derechos de dichos sujetos[2373]. Se justifica esta cesión sin consentimiento en la medida en que la excepción se recoge en la Ley orgánica de Universidades, en la que se reconoce que corresponde al Defensor Universitario velar por el respeto de los derechos y libertades de los profesores, alumnos y personal de administración y servicios[2374]. Si por esta previsión, y por la obligación que las normas disponen para todos los sujetos que forman la Universidad de auxiliar a dicha institución, se reconoce la posibilidad de

presumiblemente delictivos lo pondrá de inmediato en conocimiento del Fiscal General del Estado". CORCHETE MARTÍN, *El Defensor del Pueblo…*, cit., 2001, p. 94; CARBALLO ARMAS, *El Defensor del Pueblo…,* cit., 2003, p. 230.

[2370] "El Defensor del Pueblo acusa a Aguirre de <<vulnerar>> la Sanidad Pública", *Público,* 25 de mayo de 2009.

[2371] Artículo 22.2 LO 3/1981, 6 de abril de 1981, del Defensor del Pueblo: "*Las investigaciones que realice el Defensor del Pueblo y el personal dependiente del mismo, así como los trámites procedimentales, se verificarán dentro de la más absoluta reserva, tanto con respecto a los particulares como a las dependencias y demás organismos públicos, sin perjuicio de las consideraciones que el Defensor del Pueblo considere oportuno incluir en sus informes a las Cortes Generales. Se dispondrán medidas especiales de protección en relación con los documentos clasificados como secretos*". LUNA ABELLA, "Artículo 22…", cit., 2002, p. 570.

[2372] Artículo 33.2 LO 3/1981, 6 de abril de 1981, del Defensor del Pueblo: "*En el informe no constarán datos personales que permitan la pública identificación de los interesados en el procedimiento investigador, sin perjuicio de lo dispuesto en el artículo 24 punto uno*".

[2373] Informe jurídico de la AEPD, 0190/2005, "Cesión de datos a Defensor Universitario".

[2374] Resolución APDCM, "Petición de informe relativo a la posible cesión de datos de pacientes tratados en un determinado Servicio Médico de la Comunidad de Madrid al Defensor del Paciente de la Consejería de Sanidad y Consumo", 2005, De igual manera, se ha admitido el acceso a la información sanitaria por parte del Defensor del Paciente de la Comunidad de Madrid, cuando media en los conflictos generados en el ámbito sanitario. La justificación viene motivada porque la normativa autonómica prevé la posibilidad de que este órgano recabe la información necesaria para llevar a cabo sus funciones.

ceder datos sin autorización, parece razonable admitir que el Defensor del Pueblo, órgano reconocido expresamente en la Constitución, pueda tener acceso a determinados datos sanitarios sin recabar el consentimiento citado, en el ejercicio de sus funciones.

I.5.4.C. La cesión a compañías aseguradoras.

Otro ejemplo de cesión de datos de salud fuera del ámbito estrictamente sanitario lo constituye la transmisión de información de un paciente a una compañía aseguradora, con el fin de que quede justificado el gasto que ésta debe hacer a favor del paciente, que en la mayoría de ocasiones será bien el propio asegurado o bien un tercero perjudicado frente al que vendrá obligado a responder. Chocan aquí el derecho a la autodeterminación informativa de las personas y el interés de la empresa aseguradora a conocer tanto el coste por el tratamiento sanitario como, en su caso, las lesiones y secuelas que pudiera padecer en orden a posibles indemnizaciones.

¿Si una empresa aseguradora solicita de manera justificada a un centro el acceso a una información sanitaria de un paciente, debe dicho centro transmitir los datos requeridos? Las indicaciones en el ordenamiento respecto de esta cuestión son mínimas. La LOPD prevé la necesidad del consentimiento del titular de los datos para que las compañías aseguradoras puedan compartir los datos de salud de sus asegurados, cuando para los datos denominados comunes no es necesario dicho consentimiento[2375]. Más allá de esta referencia no aclara si es necesaria la autorización del titular para la cesión de información sanitaria a las compañías aseguradoras. Tampoco la Directiva ni la Recomendación del Consejo de Europa dan una respuesta expresa a esta cuestión.

Se puede adelantar, sin embargo, la conclusión que aquí se defiende. Se entiende que estas cesiones podrán realizarse sin necesidad de recabar el consentimiento de sus titulares. La justificación de la excepción se encuentra en el ordenamiento. La Ley sobre Responsabilidad Civil y Seguro en la Circulación de los Vehículos a Motor reconoce que el asegurador deberá satisfacer el importe del daño sufrido por el perjudicado, salvo que pruebe que el hecho que

[2375] DA sexta LOPD: "*Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados. Se modifica el artículo 24.3, párrafo 2 de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:*
"Las entidades asegurados podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.
También podrán establecer ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quien sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.
En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado"; Recomendaciónes de la Agenica de Protección de Datos en relación con el Fichero Histórico de seguros del automóvil, del que es responsable la Unión Española de Entidades Aseguradoras y Reaseguradoras, para su adecuación a la legislación vigente en materia de protección de datos, 29 de diciembre de 2001.

causa la lesión no da lugar a responsabilidad[2376]. La Ley que regula el Contrato de Seguros habilita a las empresas aseguradoras para que realicen las investigaciones pertinentes en el ejercicio de sus funciones[2377]. Resulta evidente que la obligación de satisfacer el importe del daño implica tener conocimiento previo del mismo en toda su extensión, así como las circunstancias en que se ha producido. Cuando se trate de seguros de enfermedad y asistencia sanitaria estas investigaciones llevarán a conocer información sobre la salud de las personas aseguradas. De esta manera, dichas compañías podrán conocer si el pago de la cantidad que corresponda está justificado. En la más reciente normativa sanitaria autonómica que regula el acceso a las historias clínicas se ha reconocido expresamente la posibilidad de acceso de las empresas aseguradoras a dichos documentos. El acceso deberá limitarse a los datos estrictamente necesarios a efectos de la facturación[2378]. Siguiendo esta línea interpretativa, el protocolo de actuación de algunos centros sanitarios ha suavizado la exigencia del consentimiento expreso para la cesión de la información sanitaria cuando el destinatario es la compañía aseguradora[2379]. Por su parte, si bien en alguna de sus resoluciones la AEPD no ha encontrado suficiente cobertura legal en la normativa citada[2380], en otras ha parecido seguir la interpretación que aquí se ha propuesto aplicando la excepción al consentimiento[2381]. También la jurisprudencia se ha pronunciado expresamente en algún caso en este mismo sentido[2382].

Lo cierto es que de una interpretación sistemática de la Ley de Contrato de Seguro parece deducirse la idea de que la compañía aseguradora ha de tener desde el inicio conocimiento de

[2376] Artículo 7.1 RDL 8/2004, de 29 de octubre de 2004, por el que se aprueba el texto refundido de la Ley sobre Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor: "*El asegurador, dentro del ámbito del aseguramiento obligatorio y con cargo al seguro de suscripción obligatoria, habrá de satisfacer al perjudicado el importe de los daños sufridos en su persona y en sus bienes. El perjudicado o sus herederos tendrán acción directa para exigirlo. Únicamente quedará exonerado de esta obligación si prueba que el hecho no da lugar a la existencia de responsabilidad civil conforme al artículo 1 de la presente Ley*"; Apartado I, Informe jurídico de la AEPD, "Cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios públicos", 526/2003.

[2377] Artículo 18 Ley 50/1980, de 8 de octubre, de Contrato de Seguro: *"El asegurador está obligado a satisfacer la indemnización al término de las investigaciones y peritaciones necesarias para establecer la existencia del siniestro y, en su caso, el importe de los daños que resulten del mismo. En cualquier supuesto, el asegurador deberá efectuar, dentro de los cuarenta días a partir de la recepción de la declaración del siniestro, el pago del importe mínimo de lo que el asegurador pueda deber, según las circunstancias por él conocidas.*
Cuando la naturaleza del seguro lo permita y el asegurado lo consienta, el asegurador podrá sustituir el pago de la indemnización por la reparación o la reposición del objeto siniestrado".

[2378] Artículo 15 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el Uso y Acceso a la Historia Clínica electrónica: "*A las compañías de aseguramiento privado sólo se les facilitarán aquellos datos de la historia clínica electrónica imprescindibles a efectos de facturación, con la finalidad de la justificación del gasto. Cualquier otra información clínica solicitada por la compañía aseguradora requerirá el consentimiento expreso del/de la paciente*".

[2379] Apartado 8.5.1) Código Tipo de la Agrupación Catalana de Establecimientos Sanitarios, inscrito el 28 de diciembre de 2001: cuando "*el interesado utilice los servicios sanitarios bajo la cobertura de un seguro sanitario, el establecimiento sanitario acreedor comunicará a la entidad aseguradora los datos sanitarios estrictamente necesarios para que ésta pueda conocer el acto sanitario prestado y hacer frente a su responsabilidad*". Sin embargo, considera esta agrupación que cuando el paciente desautorice expresamente esta comunicación "*el centro sanitario se abstendrá de realizarla, y ante cualquier eventual requerimiento de compañías aseguradoras al respecto, se limitará a informar de lo dispuesto por aquél. La consulta se evacuará y facturará como correspondiente a un paciente particular*".

[2380] Resolución R/00232/2008 de la AEPD, 5 de marzo de 2008, procedimiento PS/00331/2007.

[2381] Resolución R/00397/2003 de la AEPD, 11 de agosto de 2003, procedimiento PS/00027/2003; Resolución de archivo de actuaciones de la AEPD, 8 de enero de 2007. E/00164/2004. Informe jurídico de la AEPD, "Cesión de datos de salud a efectos de facturación", 114/2006. ELGUERO MERINO, "Artículo 106…", cit., 2007, p. 1.389.

[2382] SAN 22 de septiembre de 2004, FJ 2; 18 de enero de 2007, FJ 5, que señala que a pesar de que las previsiones legales no establecen de forma expresa una excepción al consentimiento, ésta se deduce del articulado de las leyes citadas.

las circunstancias que rodean a los hechos que constituyen el riesgo asegurado. Tanto la imposición al tomador del seguro del deber precontractual de declarar las circunstancias relativas al riesgo sobre su estado de salud[2383], como del deber o carga de comunicar las circunstancias que posteriormente puedan agravar dicho riesgo[2384], dejan entrever la regla general de que el asegurador debe estar informado en todo momento sobre los hechos que son objeto de protección. Esta consideración se refuerza con la idea transmitida en apartados precedentes, de que el ordenamiento parece dar cobertura a un flujo de datos entre aseguradoras, administraciones, asegurados y demás perjudicados e, incluso, centros sanitarios, que sirva de instrumento para depurar, ante un hecho determinado, las responsabilidades pertinentes en base a una adecuada información[2385]. Se subraya así la conclusión que se ha expuesto, que favorece el flujo de información entre los centros de salud y las compañías aseguradoras, para que estas últimas cuenten con todos los datos necesarios.

La previsión legal lleva a justificar la aplicación de la excepción al consentimiento. En ocasiones se han tratado de encontrar otras causas de justificación para esta excepción. Se ha planteado, por ejemplo, por alguna compañía aseguradora la posibilidad de limitar el consentimiento en la cesión de los datos sanitarios, argumentando que su actividad se dirige a prestar una asistencia sanitaria, aunque sea de forma indirecta. Como bien se ha entendido en las decisiones de la AEPD, siguiendo la jurisprudencia, este argumento carece de fundamento[2386]. La actividad de las empresas aseguradoras, incluso la que se da a través de ciertos facultativos que actúan como peritos, no se puede considerar como prestación de servicios médicos a efectos de aplicar el artículo 7.6 de la LOPD. Su actividad, en todo caso, podrá ser considerada de peritaje, dirigida no a la asistencia sanitaria, sino a evitar el pago o a

[2383] Artículo 10 Ley 50/1980, 8 de octubre de 1980, de Contrato de Seguro : "*El tomador del seguro tiene el deber, antes de la conclusión del contrato, de declarar al asegurador, de acuerdo con el cuestionario que éste le someta, todas las circunstancias por él conocidas que puedan influir en la valoración del riesgo. Quedará exonerado de tal deber si el asegurador no le somete cuestionario o cuando, aun sometiéndoselo, se trate de circunstancias que puedan influir en la valoración del riesgo y que no estén comprendidas en él (...)*". SÁNCHEZ CALERO, "Artículo 10…", cit., 2001, p. 209; REGLERO CAMPOS, "Artículo 10…", cit., 2007, p. 199.

[2384] Artículo 11 Ley 50/1980, 8 de octubre de 1980, de Contrato de Seguro: "*El tomador del seguro o el asegurado deberán, durante el curso del contrato, comunicar as asegurador, tan pronto como se sea posible, todas las circunstancias que agraven el riesgo y sean de tal naturaleza que si hubieran sido conocidas por éste en el momento de la perfección del contrato no lo habría celebrado o lo habría concluido en condiciones más gravosas*". SÁNCHEZ CALERO, "Artículo 10…", cit., 2001, p. 232; GONZÁLEZ BARRIOS, "Artículo 11…", cit., 2007, p. 259.

[2385] Artículo 25.2 RDL 8/2004, 29 de octubre de 2004, por el que se aprueba el texto refundido de la Ley Sobre Responsabilidad Civil y Seguro en la Circulación de Vehículos a Motor: *"El Consorcio de Compensación de Seguros facilitará, asimismo, al perjudicado el nombre y la dirección del propietario, del conductor habitual o del titular legal del vehículo con estacionamiento habitual en España, si aquel tuviera un interés legítimo en obtener dicha información. A estos efectos, la Dirección General de Tráfico o la entidad aseguradora proporcionará estos datos al Consorcio de Compensación de Seguros, y se establecerán, en todo caso, las medidas técnicas y organizativas necesarias para asegurar la confidencialidad, seguridad e integridad de los datos y las garantías, obligaciones y derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A la información de que disponga el Consorcio de Compensación de Seguros tendrán acceso, además de los perjudicados, los aseguradores de éstos, los organismos de información de otros Estados miembros del Espacio Económico Europeo, la Oficina Española de Aseguradores de Automóviles, en su calidad de organismo de indemnización, y los organismos de indemnización de otros Estados miembros del Espacio Económico Europeo, así como los fondos de garantía de otros Estados miembros del Espacio Económico Europeo. Tendrán también acceso a dicha información los centros sanitarios y servicios de emergencias médicas que suscriban convenios con el Consorcio de Compensación de Seguros y las entidades aseguradoras para la asistencia a lesionados de tráfico"*.

[2386] Resolución R/00232/2008 de la AEPD, 5 de marzo de 2008, procedimiento PS/00331/2007.

determinar la cuantía de la cantidad correspondiente a abonar al asegurado o perjudicado por los daños sufridos.

También se ha tratado de justificar la cesión sin consentimiento a las aseguradoras argumentando que los centros sanitarios convenidos con aquéllas son meros encargados del tratamiento, no responsables del fichero. Es decir, según esta interpretación los centros actúan en nombre y por cuenta de las aseguradoras y no como entidades que toman sus propias decisiones. Si esto fuera así no sería aplicable la regulación referente a la cesión de datos sino la relativa al acceso por parte de terceros, que luego se verá. No parece que sea necesario realizar un análisis profundo para darse cuenta que los centros sanitarios no son meros encargados que han de seguir las instrucciones de las aseguradoras. Como bien se ha explicado en alguna resolución de la AEPD, los centros sanitarios son responsables de sus propios ficheros, que manipulan la información con la finalidad de proteger la salud de sus pacientes, y no meros sujetos que sólo siguen las instrucciones de los responsables. La transmisión de los datos de éstos a compañías aseguradoras en ningún momento se puede calificar como un acceso a terceros, sino que son cesiones a todos los efectos[2387].

En algún caso la jurisprudencia se ha pronunciado al respecto de este supuesto y ha fundamentado la excepción en un argumento distinto al de la previsión legal. Concretamente, se ha basado en la existencia de una relación negocial entre el asegurador y asegurado, para justificar el acceso a los datos sanitarios sin necesidad de recabar el consentimiento del titular de los datos[2388]. El sujeto particular firma un contrato con la empresa aseguradora para cuyo desarrollo es necesario, muchas veces, el tratamiento de los datos sanitarios. Según el argumento defendido por los tribunales, la posibilidad de que el sujeto asegurado o lesionado se niegue a la citada transmisión de datos haría inviable que la compañía aseguradora pudiera desarrollar su labor con las garantías necesarias. La prohibición, por parte del titular, de la transmisión de los datos sanitarios convertiría las previsiones legales contenidas en la normativa sobre los contratos de seguros en meras declaraciones programáticas[2389]. La posición jurisprudencial precedente es cuestionable en base a argumentos que ya se han dado. La aplicación de la excepción al consentimiento por motivo de la existencia de una relación negocial está prevista en la LOPD en la regulación de las cesiones de los datos comunes[2390]. Como se ha repetido aquí, y se ha recogido en algún informe de la AEPD, este régimen genérico no es aplicable a los datos sanitarios[2391]. La regulación común no se aplica automáticamente a la cesión de este tipo de información, que es considerada merecedora de una protección especial.

[2387] Resolución R/00232/2008 de la AEPD, 5 de marzo de 2008, procedimiento PS/00331/2007. Informe jurídico de la AEPD, "Cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios privados", 359/2002.
[2388] SAN 18 de enero de 2007, FFJJ 3 y 5.
[2389] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, pp. 94-95.
[2390] Artículo 11.2.c) LOPD.
[2391] Informe jurídico de la AEPD, "Acceso por parte de las Mutualidades Administrativas a datos recogidos por centros sanitarios", 0369/2005: "es necesario analizar si la cesión de los datos a las Mutualidades y su posterior tratamiento por aquéllas se encontrará habilitado por una norma con rango de Ley, tal y como exige el artículo 7.3 de la Ley Orgánica 15/1999, al no ser posible aplicar a los datos de salud ninguna de las habilitaciones para el tratamiento y la cesión de los datos contempladas en los artículos 6 y 11 de la Ley Orgánica 15/1999"; Apartado III Informe jurídico de la AEPD, "Cesión de datos de salud a aseguradoras de asistencia sanitaria por profesionales de la medicina", 449/2004.

En una línea parecida a la que se acaba de exponer, se ha planteado la posibilidad de entender que cuando una persona se vincula a una aseguradora mediante un contrato está prestando su consentimiento expreso, para que se trasladen los datos sanitarios a esta compañía[2392]. Esta consideración tendría sentido si el citado contrato incorporara una cláusula en la que se especifica la facultad de la compañía aseguradora de acceder a los datos sanitarios del asegurado y el afectado diera su consentimiento expreso sobre dicha facultad concreta. Si la autorización del titular de los datos no recae sobre este objeto determinado, difícilmente podrá entenderse que existe un consentimiento expreso[2393]. Podría hablarse, quizás, de autorización presunta o como mucho tácita, pero, como es conocido, este tipo de consentimiento no se acepta cuando se trata de manipular datos relativos a la salud de las personas.

En definitiva, la excepción al consentimiento se fundamenta aquí en el hecho de que las leyes así lo prevén. Más allá de las interpretaciones que se puedan dar a la hora de resolver la colisión de intereses que se plantea y del fundamento que se emplee para argumentar la aplicación de la excepción, es necesario volver a subrayar que el criterio de proporcionalidad ha de guiar el conflicto de intereses que se plantea. Se ha entendido que la justificación a la excepción del consentimiento viene dada fundamentalmente porque las leyes prevén dicho supuesto exceptuado. Sin embargo, si bien el límite al consentimiento puede tener aplicación por previsión legal, en beneficio del principio de proporcionalidad será necesario respetar determinadas garantías dirigidas a salvaguardar mínimamente el derecho a la autodeterminación informativa. Así, por un lado, sólo serán transmitidos por los centros los datos relativos a la cualidad de las lesiones y actos de asistencia llevados a cabo[2394] y, por otro, deberá informarse al asegurado o perjudicado sobre tal comunicación.

I.5.4.D. La cesión de datos sanitarios a los medios de comunicación.

I.5.4.D.a. Criterio a aplicar para resolver la colisión entre el derecho a la autodeterminación informativa y la libertad de información.

Otro supuesto de cesión o revelación de datos de carácter personal sanitarios puede ser el que se lleve a cabo a favor de los medios de comunicación[2395]. Se trata del caso en que estos medios acceden a los datos de salud para después, en ejercicio del derecho a informar, sacarlos a la luz por considerarlos de relevancia pública. Es conocido que en ejercicio de la libertad de información numerosos datos se recaban para ser transmitidos después al público[2396]. Más allá de que la publicación de esta información por los medios pudiera constituir o no una vulneración de la intimidad, no se puede negar que el mero acceso a los datos supone en sí mismo un tratamiento de datos en términos de la LOPD que ha de analizarse desde la perspectiva del derecho a la autodeterminación informativa. Siendo esto así, la manipulación de información

[2392] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 97.
[2393] SAN 9 de julio de 2009, FJ 3, en el que se resuelve el supuesto en que una aseguradora accede a datos de salud de un sujeto que había consentido expresamente dicho acceso. Informe jurídico de la AEPD, "Cesión de datos de salud a aseguradoras de asistencia sanitaria por centros sanitarios privados", 359/2002.
[2394] VIGUERAS PAREDES, "Comunicar Datos...", cit., 2004.
[2395] VERDÚ PASCUAL, *Secreto Profesional…,* cit., 2005, p. 31, pone de manifiesto cómo es común que los medios de comunicación informen sobre aspectos clínicos de deportistas profesionales.
[2396] ARIAS MÁIZ, "Una excepción al principio…", cit., 2010, p. 560.

deberá cumplir con los requisitos que exige la normativa de protección de datos, fundamentalmente, el deber de informar y el derecho a consentir.

Esta manipulación ha adquirido hoy día, con la incorporación de las TIC, una nueva dimensión[2397]. El denominado caso Miterrand pone de manifiesto este hecho. La difusión por estos medios de los detalles de los últimos momentos de la vida del presidente francés, hizo que el secuestro decretado por los órganos judiciales franceses de la publicación en formato papel de la misma información, por considerar que atentaba contra la intimidad, careciera de efectos prácticos. La información ya había sido puesta en común a través de la Red[2398].

Este caso refleja el hecho de que las nuevas tecnologías multiplican el riesgo que las cesiones generan y las dificultades de controlar el flujo de datos en el ciberespacio, lo cual hace realmente difícil preservar el derecho a la intimidad y autodeterminación informativa, si no es a través de la actuación judicial a posteriori. No se quiere hacer en este momento un estudio extenso sobre el régimen jurídico del derecho a la información. Bastará con acercarse a esta figura para entender la confrontación de intereses que se indica.

Las normas no han entrado a regular expresamente esta problemática. Una de las pocas referencias se encuentra en la Directiva europea que, tras reconocer la necesidad de limitar el derecho a la autodeterminación informativa para favorecer el ejercicio del derecho a la libertad de información, no hace más que una remisión a la normativa interna de cada Estado[2399]. Este precepto de la norma europea ha sido interpretado por el Grupo de Trabajo creado al amparo del artículo 29 de la propia Directiva, si bien este organismo se ha limitado a poner de manifiesto la particularidad del conflicto jurídico expuesto y a hacer un llamamiento general a que se aplique con rigor el principio de proporcionalidad en cada caso en que se produzca el choque entre el derecho a la autodeterminación informativa y la libertad de información[2400]. Por su parte, el Convenio del Consejo de Europa para la protección de las personas respecto al tratamiento

[2397] CORREDOIRA Y ALFONSO, "Internet (II)…", cit., 2003, p. 561; ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, p. 37; SANJURJO REBOLLO, *Manual de Derecho…,* cit., 2009, p. 161.

[2398] FERNÁNDEZ ESTEBAN, "El Impacto...", cit., 1999, pp. 528-529.

[2399] Considerando 37 Directiva 95/46/CE: "*Considerando que para el tratamiento de datos personales con fines periodísticos o de expresión artística o literaria, en particular en el sector audio-visual, deben preverse excepciones o restricciones de determinadas disposiciones de la presente Directiva siempre que resulten necesarias para conciliar los derechos fundamentales de la persona con la libertad de expresión y, en particular, la libertad de recibir o comunicar informaciones, tal y como se garantiza en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales; que por lo tanto, para ponderar estos derechos fundamentales, corresponde a los Estados miembros prever las excepciones y las restricciones necesarias en lo relativo a las medidas generales sobre la legalidad del tratamiento de datos, las medidas sobre la transferencia de datos a terceros países y las competencias de las autoridades de control sin que esto deba inducir, sin embargo, a los Estados miembros a prever excepciones a las medidas que garanticen la seguridad del tratamiento; que, igualmente, debería concederse a la autoridad de control responsable en la materia al menos una serie de competencias a posteriori como por ejemplo publicar periódicamente un informe al respecto o bien iniciar procedimientos legales ante las autoridades judiciales.* Artículo 9 Directiva 95/46/CE: "*Tratamiento de datos personales y libertad de expresión.*

En lo referente a l tratamiento de datos personales con fines exclusivamente periodísticos o de expresión artística o literaria, los Estados miembros establecerán, respecto de las disposiciones del presente capítulo, del capítulo IV y del capítulo VI, exenciones y excepciones sólo en la medida en que resulten necesarias para conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión".

[2400] Recomendación del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/97, "La normativa sobre protección de datos y los medios de comunicación", de 25 de febrero de 1997.

automatizado de datos dispone que no se requiere el consentimiento del titular, para el tratamiento de datos que se dirija a la protección de los derechos y libertades de otras personas[2401]. Evidentemente, entre estas libertades se encuentra la libertad de información. La normativa interna no hace referencia a este supuesto concreto[2402]. Ni la LOPD ni el reglamento que la desarrolla regulan este aspecto. Esto no ha evitado, sin embargo, que en otras instancias se reconozca que en la práctica es posible la colisión entre el derecho a la autodeterminación informativa y la libertad de información, y que es necesaria la regulación de este conflicto. En este sentido, la jurisprudencia ha señalado que si bien las normas de protección civil del derecho al honor, intimidad e imagen otorgan un importante ámbito de protección de las personas frente a los medios que ejercen la libertad de información, es necesario también analizar el ejercicio de la libertad de información desde la perspectiva del derecho a la autodeterminación informativa. Es innegable que la libertad de información puede afectar al referido derecho[2403]. Por lo tanto, es necesario que se aporten instrucciones sobre cómo interpretar la colisión entre estos intereses. Si bien la normativa de protección de datos interna no regula expresamente esta cuestión, la jurisprudencia ha aportado criterios que han de ser puestos de manifiesto.

Como ya se vio al analizar el principio de veracidad, tanto la doctrina como la jurisprudencia han reconocido que el respeto a la libertad de información se erige en derecho fundamental de cualquier Estado considerado democrático[2404], incluso como medio para hacer efectivos otros derechos, caso de la libertad ideológica[2405]. Es sabido que promover un adecuado flujo de información es instrumento indispensable en orden a garantizar una opinión pública libre[2406]. La libertad de información, entendida como el derecho a una comunicación pública libre, constituye una garantía institucional reconocida en la Constitución[2407]. El acceso de los ciudadanos a una información veraz garantiza que los individuos que conforman la sociedad puedan valorar los diferentes aspectos de la realidad.

Sin duda, para que los ciudadanos puedan recibir esta información será necesario que los medios de comunicación tengan acceso a datos, que la mayoría de las veces conciernen a personas físicas. Este acceso afectará a diferentes derechos fundamentales. La Constitución reconoce expresamente en la intimidad un límite al derecho a la información[2408], pero más allá de este derecho, también la autodeterminación informativa puede verse afectada[2409]. En concreto,

[2401] Artículo 9.2.b) Convenio 108/1981 del Consejo de Europa.
[2402] SAN 12 de enero de 2001, FJ 4, apunta el hecho de que en el Estado no existe una regulación concreta dirigida a cohonestar el tratamiento de datos de carácter personal y la libertad de información.
[2403] SAN 1 de octubre de 2008, FJ 5; STJUE 16 de diciembre de 2008, Tietosujavaltuutettu v. Satakunnan Markkinapörssi Oy y otros, en la que se contraponen el derecho a la libertad de información y la autodeterminación informativa, al publicar un medio de comunicación datos fiscales de multitud de ciudadanos.
[2404] TORRES DEL MORAL, "La Libertad de Comunicación…", cit., 2002, p. 23; ORTEGA GUTIÉRREZ, *Manual de Derecho…*, cit., 2003, p. 22.
[2405] ORTEGA GUTIÉRREZ, *Manual de Derecho…*, cit., 2003, pp. 37-41.
[2406] STC 14 de febrero de 1992, FJ 3. SÁNCHEZ FÉRRIZ, "El Derecho de la Información…", cit., 2003, pp. 36-37; ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, pp. 54-55 y p. 369.
[2407] Artículo 20 CE. STC 12 diciembre de 1986, FJ 6; STEDH 27 de marzo de 1996, Goodwin v. Reino Unido, apartado 39. URÍAS, *Lecciones de Derecho…,* cit., 2003, p. 57.
[2408] Artículo 20.4 CE: "*Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia*". GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* 2007, pp. 64-66.
[2409] SAN 16 de marzo de 2006, FJ 5. LESMES SERRANO, "Artículo 1…", cit., 2008, p. 58.

los datos de salud pueden resultar objeto de manipulación por parte de los medios de comunicación con el fin de informar a los ciudadanos sobre determinados hechos. En algún caso los tribunales han analizado el conflicto generado entre la libertad de informar de un periodista y el derecho a la intimidad de unos reclusos, por haber publicado el primero información sobre el estado de salud de estos últimos, que se encontraban afectados por el SIDA[2410]. También la AEPD ha resuelto supuestos semejantes, en que este tipo de información se manipula por los medios[2411].

En relación al conflicto que se crea entre el derecho a la intimidad y la libertad de información el Tribunal Constitucional ha establecido unos criterios bien definidos para resolverlo[2412]. Sin embargo, no parece que se haya aportado un criterio específico cuando lo que entra en juego es el derecho a la autodeterminación informativa[2413]. Se entiende que para estos casos será aplicable el criterio seguido cuando es la intimidad el derecho afectado. Esta interpretación encuentra apoyo en diferentes fuentes. Por un lado, la Directiva europea reguladora de la protección de datos se refiera expresamente al derecho a la intimidad, como bien jurídico que colisiona con la libertad de expresión, cuando atiende al conflicto de intereses que ahora se analiza. La referencia a la intimidad podría entenderse como un llamamiento a aplicar en el ámbito de la protección de datos los criterios aplicados para solucionar el conflicto entre la intimidad y la libertad de información. En esta misma línea alguna resolución de la AEPD ha analizado los criterios citados para resolver la colisión entre la libertad de información y la intimidad, para resolver la confrontación producida entre la libertad de información y la autodeterminación informativa[2414]. Así se hace también en la jurisprudencia que, aunque en contadas ocasiones, se ha enfrentado a este conflicto. En algún caso especialmente polémico, por el trato que se le ha dado en los medios de comunicación[2415], y también en otros supuestos[2416], los criterios que se han aplicado son los utilizados en numerosas ocasiones por el TC para decidir en relación a la colisión entre la intimidad y la libertad de información[2417]. El

[2410] STS 18 de febrero de 1999. En el mismo sentido STEDH 25 de noviembre de 2008, Armoniené v. Lithuania, FFJJ 42-48

[2411] Resolución de la APDCM, "Se archiva un procedimiento iniciado contra un hospital de la Comunidad de Madrid en relación con la publicación en un medio de comunicación de datos relativos a un paciente que había sufrido un accidente".

[2412] ESCOBAR DE LA SERNA, *Derecho de la Información…,* cit., 2004, pp. 426-427.

[2413] ATC 18 de mayo de 2009, FJ 3, reconoce que no hay criterios definidos para resolver la colisión entre el derecho a la autodeterminación informativa y la libertad de información.

[2414] Resolución de la AEPD, expediente nº E/00949/2007, 9 de mayo de 2008.

[2415] Juzgado de Primera Instancia de Madrid 18 de diciembre de 2009, en la que se resuelve el caso en que un medio de comunicación "cuelga" o publica en Internet un listado de personas identificables y su afiliación a un determinado partido político. Esta decisión ha sido revisada por SAP de Madrid 11 de junio de 2010.

[2416] SSAN 12 de enero de 2001, FJ 4, 8 de julio de 2009, FFJJ 4 y 5 y 9 de julio de 2009, FJ 4; STS 26 de junio de 2008, FJ 2; STC 28 de enero de 2003, FFJJ 7 y 8, en la que se analiza la entrega de una fotografía por parte de las Fuerzas de Seguridad a los medios de comunicación, señalando que también el derecho a la autodeterminación informativa puede verse lesionado con esta acción. Para resolver la colisión se emplean los mismos criterios utilizados que cuando se ve afectado el derecho a la intimidad.

[2417] COTINO HUESO, "Datos personales…", cit., 2010, pp. 311-312.

derecho comparado también da argumentos a favor de este criterio[2418]. Lo mismo se ha predicado desde la escasa doctrina que se ha pronunciado al respecto[2419].

Según el TC la colisión entre la libertad de información y el derecho a la intimidad se soluciona en base al siguiente criterio: más allá de los requisitos generales que ha de cumplir todo límite a un derecho fundamental, entiende el tribunal que prevalecerá la libertad de información sobre el derecho a la intimidad cuando la información que se divulgue a través del medio de comunicación tenga relevancia pública[2420]. La casuística que rodea a este asunto es abundante y los matices que puede presentar cada caso llevarían a tener que realizar un trabajo que sobrepasaría el objeto del estudio que aquí se pretende[2421], por lo que se realizará simplemente una breve exposición sobre cuándo se entiende que una información cuenta con relevancia pública.

I.5.4.D.b. Sobre cuándo una información cuenta con relevancia pública.

Lo fundamental, por lo tanto, es determinar cuándo una información resulta de relevancia pública. Dar una definición de lo que se considera de relevancia pública es especialmente complejo, pues se trata de una realidad relativa cuyo sentido depende de las circunstancias en las que se analice: su contenido cambia dependiendo del momento histórico o el lugar en que se produzca su estudio[2422]. En todo caso, la relevancia pública de una información derivará de la condición bien de los hechos o bien de la persona a la que se refiere[2423].

A) En relación a los hechos, su relevancia pública resulta de que su contenido sea de "interés público o general", es decir de que se refiera a acontecimientos que interesan al conjunto de la sociedad[2424]. Estos hechos se diferencian de los que afectan a los intereses particulares. Sobre todo se distinguen de aquéllos que son simplemente del "interés del público"[2425]. El concepto de interés público no coincide con el de interés del público. El interés del público puede ir dirigido a conocer información que tiene más que ver con el morbo o la curiosidad, que con hechos que ayudan a comprender mejor la realidad que objetivamente guarda dicho interés[2426]. De inicio, se considera que cuando la información va dirigida, simplemente, a satisfacer la mera curiosidad de las personas esta información carece del citado interés público[2427]. Por ejemplo, se ha interpretado que comunicar información sobre la salud de una menor portadora de anticuerpos

[2418] KUKK, *"Los medios de comunicación…",* cit., 2007, en la que se hace referencia al caso estonio, donde la reciente Ley de Protección de Datos hace depender la prevalencia de la libertad de información al hecho de que la información sea de relevancia pública o interés general.
[2419] ARIAS MÁIZ, "Una excepción al principio…", cit., 2010, p. 570.
[2420] SSTC 14 de febrero de 1992, FJ 3; 22 de abril de 2002, FJ 5. URÍAS, *Lecciones de Derecho…,* cit., 2009, pp. 200-201.
[2421] COTINO HUESO, "Datos personales…", cit., 2010, pp. 313-: apunta una serie de supuestos en que se analiza si existe interés público o no, en la información que se transmite, para ver si la libertad de información se impone al derecho a la autodeterminación informativa.
[2422] URÍA, *Lecciones de Derecho…,* cit., 2009, p. 116.
[2423] STC 22 febrero de 1989, FJ 2.
[2424] STC 15 julio de 1999, FJ 8. URÍA, *Lecciones de Derecho…,* cit., 2009, p. 116.
[2425] MIERES MIERES, *Intimidad Personal…*, cit., 2002, p. 69.
[2426] STS 11 de noviembre de 2004, FJ Único.
[2427] STC 14 de febrero de 1992, FJ 3. LAZCANO BROTONS, "Comentario al artículo 10…", cit., 2009, p. 478. SANJURJO REBOLLO, *Manual de Derecho…,* cit., 2009, p. 82.

del Sida, identificándola y sin obtener las autorizaciones pertinentes, no reviste relevancia social, pues la vida privada de la niña no es per se de interés general[2428]. Se podría concluir que una información será de interés público cuando, lejos del mero morbo, ayuda a tener una visión más completa de la realidad que afecta al conjunto de la ciudadanía[2429]. Son claro ejemplo de hechos que cuentan con relevancia pública los acontecimientos referidos a investigaciones de carácter penal[2430]. Más allá de estas definiciones generales, los tribunales han ido analizando caso por caso qué situaciones o realidades pueden considerarse de relevancia pública. El análisis debe hacerse atendiendo al contenido de la información, el contexto en que se remite y considerando si para transmitir el mensaje que se pretende trasladar es necesario comunicar determinados datos. Por ejemplo, se ha entendido que la información sobre la violación de una persona y la captura del presunto agresor es de relevancia pública, pero que, sin embargo, las referencias a la identidad de la persona agredida sexualmente y a su virginidad no eran necesarias para transmitir el mensaje pretendido[2431].

B) La relevancia pública puede derivar también de la condición de la persona a la que se refiere la información[2432]. Cuando se trata de personajes públicos o de relevancia pública la confrontación entre los derechos que ahora entran en juego adquiere otra dimensión. Cuando se habla de este tipo de sujetos se está haciendo referencia a cargos públicos, personas que son conocidas debido a su trabajo, o personas que adquieren notoriedad pública debido a que acostumbran a exponer aspectos de su vida al público. Se entiende que este tipo de personas han de sufrir mayores intromisiones en su vida privada. Su derecho a la intimidad se encuentra más limitado[2433]. Esto no quiere decir que no cuenten con dicho derecho[2434]. El mero hecho de que alguien tenga relevancia pública no supone que todos los datos que le conciernen la tienen[2435]. Se considera que, más allá de la esfera abierta al público, incluso los sujetos con notoriedad pública guardan una esfera privada a la que no se puede tener acceso[2436]. En principio, solamente los hechos relacionados a los factores que hacen que este sujeto tenga relevancia pública se constituyen de interés público[2437]. Sobre los demás hechos la libertad de información debería ceder a favor de la intimidad. En este sentido, también cuando la información publicada se refiere a personas de relevancia pública lo realmente importante resulta analizar el contenido de los hechos transmitidos[2438]. Esta situación se plantea, por ejemplo, en referencia a

[2428] STC 7 de marzo de 2006, FJ 3.
[2429] GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* 2007, p. 285.
[2430] STC 25 de febrero de 2002, FJ 8; 4 de junio de 2007, FJ 8, en la que se considera de relevancia pública una información emitida sobre la desaparición de una persona. MEDINA GUERRERO, *La Protección Constitucional…,* cit., 2005, p. 134.
[2431] STC 14 de octubre de 2002, FJ 4. En el mismo sentido, la conocida STC 12 de julio de 1993, FJ 4, en la que se entiende que dar información sobre el asesinato de unas personas se considera relevante, no así transmitir datos sobre la salud y cuidados que recibe en sus partes íntimas uno de los sujetos implicados en el caso, pues esta información no aporta nada en relación a los asesinatos.
[2432] SÁNCHEZ FERRIZ, *Delimitación de las libertades…,* cit., 2004, p. 187; GARBERÍ LLOBREGAT, *Los Procesos Civiles…,* 2007, p. 287; LAZCANO BROTONS, "Comentario al artículo 10…", cit., 2009, p. 479.
[2433] STC 17 de octubre de 1991 FJ 4. MEDINA GUERRERO, *La Protección Constitucional…,* cit., 2005, p. 144.
[2434] SANJURJO REBOLLO, *Manual de Derecho…,* cit., 2009, p. 82. STC 22 de mayo de 1995, FJ 2.
[2435] SSTC 17 de octubre de 1991 FJ 4; 22 de abril de 2002, FJ 5.
[2436] STC 5 de mayo del 2000, FJ 9. ESCOBAR DE LA SERNA, *Derecho de la información…,* cit., 2004, p. 428; SANTOS VIJANDE, *La Protección Jurisdiccional…,* cit., 2005, pp. 154-155.
[2437] STEDH 24 de junio de 2004, Von Hannover v. Alemania, FFJJ 63-67.
[2438] URÍA, *Lecciones de Derecho…,* cit., 2009, p. 120.

quienes tienen atribuida la administración del poder público. En estos casos se entiende que son personajes públicos, de manera que su actividad se encuentra sometida al escrutinio público. Cuando la información publicada se refiera al ejercicio del cargo de interés general el afectado no podrá oponer el derecho a su intimidad. Por el contrario, cuando la información afecta a aspectos que nada tienen que ver con el ejercicio de ese cargo público, la intimidad podrá ser alegada[2439].

En lo que corresponde a las personas con notoriedad pública, que no son cargos públicos, sino sujetos que adquieren esa relevancia por su profesión o porque acostumbran a difundir aspectos de su vida, ocurre lo mismo. Es el caso, por ejemplo, en que un personaje de notoriedad pública, cuya vida privada ha sido hecha pública en numerosas ocasiones, ve su intimidad vulnerada por el hecho de que un medio de comunicación hace pública información sobre su vida sexual[2440]. En estos supuestos, sin embargo, cuando se trata de personas que divulgan su vida privada el margen de actuación a la hora de revelar datos es mayor[2441]. Hay que tener en cuenta, en todo caso, que la actuación previa del propio sujeto de relevancia pública destapando determinados aspectos de su vida privada, y haciéndolos públicos, condicionará a futuro el alcance de su derecho a la vida privada[2442]. Por ejemplo, una persona que había adoptado un menor y había hecho pública determinada información sobre el proceso de adopción, alegó que su intimidad había sido vulnerada porque unos medios habían publicado determinados datos sobre el mismo proceso de adopción. Los tribunales, si bien en última instancia dieron la razón al personaje público, reconocieron que el hecho de que anteriormente dicha persona hubiera hecho públicos datos sobre los hechos condicionó el contenido de la decisión que se tomó[2443].

El criterio que se acaba de citar, y que se emplea para resolver el enfrentamiento entre la libertad de información y el derecho a la intimidad, puede ser utilizado con el fin de resolver el conflicto que aquí se analiza entre la libertad de información y el derecho a la autodeterminación informativa. El acceso de los medios de comunicación a la información sanitaria de un ciudadano estará justificado siempre y cuando esta información tenga relevancia pública. La relevancia vendrá porque el hecho en sí guarda esta importancia o porque el sujeto al que se refiere tiene dicha relevancia.

El hecho podrá tener relevancia pública cuando afecte al interés general. La relevancia pública en hechos vinculados al ámbito de la salud puede verse, por ejemplo, en el supuesto en que la salud pública está en juego por determinada enfermedad, o en el caso en que se cuestiona el buen funcionamiento de un determinado sistema sanitario. En estos casos los medios de comunicación tienen que tener acceso a cierta información para, después, comunicar estos datos de indudable interés social al público.

[2439] STC 25 de octubre de 1999, FJ 7.
[2440] STC 6 de mayor de 2002, FJ 8.
[2441] MEDINA GUERRERO, *La Protección Constitucional…,* cit., 2005, p. 153.
[2442] STS 25 de febrero de 2009, FJ 2.
[2443] STC 15 de julio de 1999, FJ 7, en la que se da la razón al personaje público, si bien por el hecho de que la intimidad vulnerada ha sido la del menor adoptado, no la del personaje público que había sacado la información a la luz.

El que tengan derecho a acceder a una información de relevancia pública no significa, sin embargo, que ese ejercicio pueda ser ilimitado. Estando justificado el acceso deberá analizarse si es necesario en el caso particular que los medios conozcan la identidad de las personas titulares de los datos a los que se pretende acceder. Habrá que ver, una vez más, si para cumplir el fin pretendido, informar, es necesaria la asociación entre datos e identidad de sus titulares. En los casos que aquí se analizan difícilmente puede justificarse el acceso a la identidad de los enfermos[2444]. Para informar sobre una epidemia, siguiendo el ejemplo citado, no será necesario acceder a la identidad de los pacientes afectados por la misma, por lo que la publicación de ese dato sólo podrá realizarse si se obtiene el consentimiento del titular. Lo relevante será el hecho en sí, no la identidad de las personas afectadas por el mismo. Parece evidente que tratar de informar en estos supuestos al público sobre las circunstancias personales de un enfermo sin su consentimiento, sólo responde a la curiosidad, nunca al interés general[2445]. En definitiva, el acceso por los medios a información sanitaria vinculada a hechos cuyo conocimiento puede ser de interés común encontrará, la gran mayoría de las veces, un límite en la necesidad de disociar los datos. No será imprescindible que estos medios accedan a la identidad de los usuarios del sistema sanitario.

Otra cosa sucede cuando se trata de informar sobre la salud de una persona de relevancia pública. Como se ha afirmado, estos sujetos ven su derecho a la intimidad restringido, en relación al mismo derecho ejercido por simples particulares. Sin embargo, el acceso de los medios de comunicación a la información sanitaria de estos personajes sólo podrá justificarse en cierta medida. En la mayoría de casos es necesario que la información se refiera a hechos que tienen que ver con elementos que conciernen a los motivos por los que la persona es conocida. Es decir, sigue siendo necesario que dicha información responda a un interés público. Sólo cuando los datos conciernen a personas de notoriedad pública, que acostumbran a hacer pública su vida privada, el margen de actuación puede ser mayor. La jurisprudencia analiza caso por caso cuándo trasciende esta relevancia, interpretando las características de cada persona.

En conclusión, la colisión entre la libertad de información ejercida por los medios de comunicación y el derecho a la autodeterminación informativa, que puede producirse en la medida en que dichos medios quieren acceder a determinados datos, deberá resolverse atendiendo a las características de los hechos o de las personas sobre las que se pretende informar y analizando si dicha información cuenta con relevancia pública.

I.5.4.E. El uso de datos sanitarios con fines policiales.

I.5.4.E.a. Acercamiento al marco normativo que regula este supuesto de cesión.

Las Fuerzas y Cuerpos de Seguridad tienen como función principal la investigación de los delitos y, en términos generales, el mantenimiento de la seguridad pública. Tanto los cuerpos que

[2444] STS 18 de febrero de 1999, FJ 6. Juzgado de Primera Instancia de Madrid 18 de diciembre de 2009, FJ 4: "considera el Tribunal que (…) lo noticiable no era la afiliación de determinadas personas, revelando sus datos (nombre, apellidos e, incluso, domicilio), al citado partido sino y en cualquier caso la mera denuncia de irregularidades en la afiliación en la localidad de Villaviciosa de Odón".
[2445] STC 14 de febrero de 1992, FJ 3.

actúan a nivel estatal, como las policías autonómicas y locales, dentro de su ámbito competencial, dirigen su actividad al cumplimiento de dichas finalidades[2446]. Para hacer efectivos estos objetivos llevan a cabo actividades tanto administrativas, como estrictamente policiales. Interesan aquí las segundas, en la medida en que las cesiones a favor de los cuerpos de seguridad se realizarán con fines estrictamente policiales[2447]. Es conocido que en el ejercicio de estas funciones resulta necesario que los agentes accedan a la mayor información posible[2448]. Hoy día, por ejemplo, cada vez se pone más de manifiesto la relevancia del acceso de los agentes policiales a muestras biológicas, como medio para extraer información sobre la identidad de posibles infractores[2449]. En ocasiones, el cumplimiento de sus funciones requerirá que las policías se hagan con datos de carácter sanitario. Se plantea ahora si ese acceso exige el consentimiento del titular o no. ¿Pueden los centros sanitarios ceder esos datos a la policía sin que medie autorización del titular?

En relación al tratamiento de datos por las Fuerzas y Cuerpos de Seguridad la LOPD dispone en su artículo 22.2, con rango de Ley ordinaria[2450], que *"la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad".* En lo que concierne a los datos relativos a la salud de las personas, y en general a los datos considerados por la Ley como especialmente protegidos, el apartado tercero del artículo 22 de la LOPD señala que "*la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la*

[2446] Artículos 37 y 38 LO 2/1986, 13 de marzo de 1986, de Fuerzas y Cuerpos de Seguridad, donde se regula las Competencias de las Policías de las Comunidades Autónomas. Artículo 17 Estatuto CAPV. Artículo 51 LO 2/1986, 13 de marzo de 1986, de Fuerzas y Cuerpos de Seguridad, donde se recoge el funcionamiento y las competencias de la Policía Local. Artículo 25.2 LBRL. ANTÓN BARBERÁ y SOLER TORMO, *Administración Policial,* cit., 2000, p. 177 y siguientes.

[2447] CASADO CADARSO y VILA MUNTAL, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.391; ZAMORA JIMÉNEZ, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.409, analizan los ficheros policiales con fines administrativos.

[2448] AGUADO I CUDOLA, *Derecho de la Seguridad Pública…,* cit., 2007, p. 156.

[2449] STS 4 de octubre de 2006, FJ 1, en el que se autoriza el acceso de las Fuerzas y Cuerpos de Seguridad a la información resultante del análisis de una muestra de saliva extraída de una colilla. STEDH 4 de diciembre de 2008, S. and Marper v. Reino Unido, FFJJ 113-126, en la que se concluye que si bien el uso de estas herramientas puede ser útil en la lucha, por ejemplo, contra el terrorismo, deberá hacerse de acuerdo al principio de proporcionalidad. De esta forma, entiende el Tribunal que el almacenamietno permanente de información extraída empleando estos medios por parte de las Fuerzas y Cuerpos de Seguridad no está justificado cuando se trata de personas que han sido sospechosas en un procedimiento de investigación, pero no condenadas.

[2450] Disposición Final Segunda LOPD. Ya se ha puesto de manifiesto a lo largo de este trabajo que los límites a los derechos fundamentales han de ser fijados, de inicio, mediante Ley orgánica. Podría pensarse que las disposiciones que ahora se estudian son el desarrollo de otras que tienen rango de Ley orgánica. No obstante, no se acerca a ver qué artículos pueden constituir ese marco, más general, en el que se podrían basar los preceptos que ahora se analizan. Es por ello que puede criticarse el hecho de que un artículo que reconoce una limitación al derecho a la autodeterminación informativa, referida en este caso, además, a información especialmente relevante como es la sanitaria, se reconozca en una Ley ordinaria.

obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales"[2451]*.* De la lectura de este último artículo no se desprende que los datos relativos a la salud de las personas pueden cederse sin el consentimiento de sus titulares cuando la finalidad es la investigación policial. Sin embargo, de una interpretación sistemática del ordenamiento podrá llegarse a dicha conclusión.

La Directiva europea no dispone expresamente que los datos relativos a la salud de las personas puedan ser manipuladas sin el consentimiento del titular para alcanzar los mencionados fines, no obstante, abre la puerta para que en el ámbito estatal pueda recogerse una excepción de dicha naturaleza[2452]. En lo que toca directamente a los datos de carácter sanitario, el Consejo de Europa ha fijado unas claves que pueden ayudar a comprender mejor esta cuestión. Partiendo de lo que ya dispuso en el Convenio de 1981[2453], la Recomendación sobre la protección de datos médicos señala que los datos sanitarios pueden comunicarse, siempre que una Ley así lo prevea, sin el consentimiento del titular, cuando la finalidad de dicha operación sea la prevención de un peligro real o la represión de un delito específico[2454]. La memoria explicativa de esta recomendación viene a confirmar expresamente la posibilidad de manipular los datos sanitarios sin el consentimiento del titular con los citados fines de carácter policial[2455].

Más allá de la normativa que regula la protección de datos de carácter personal, las leyes que determinan la organización y funcionamiento de las Fuerzas y Cuerpos de Seguridad parecen habilitar a estos órganos para acceder a los datos de carácter personal oportunos. Las normas que determinan las funciones de estos organismos reconocen la necesidad de que lleven a cabo las acciones necesarias para la investigación y prevención de las infracciones[2456].

[2451] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...*, cit., 2001, sobre el tratamiento de los datos de carácter personal con fines policiales.

[2452] Artículo 8.4 Directiva 95/46/CE: "*Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control*". Considerando 43 Directiva 95/46/CE: "*Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa*".

[2453] Artículo 9.2.a) Convenio 108/1981 del Consejo de Europa: "*Será posible una excepción en las disposiciones de los artículos 5,6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática: a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales".*

[2454] Artículo 7.3 R (97) 5: "*Los datos médicos pueden comunicarse si son relevantes y:*
a. si la comunicación está prevista por la ley y constituye una medida necesaria en una sociedad democrática por: (...) ii. la prevención de un peligro real o la represión de un delito específico

[2455] Punto 78, Memoria Explicativa Recomendación R (97) 5 del Consejo de Europa.

[2456] Artículo 11.1 LO 2/1986, 13 de marzo, de Fuerzas y Cuerpos de Seguridad: "*Las Fuerzas y Cuerpos de Seguridad del Estado tienen como misión proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana mediante el desempeño de las siguientes funciones: g) Investigar los delitos para descubrir y detener a los*

La jurisprudencia no ha entrado a determinar expresamente la posibilidad de ceder los datos sanitarios a estos órganos. Sin embargo, de sus decisiones parece resultar que esta operación está plenamente permitida. En concreto el TEDH ha marcado en su jurisprudencia una línea interpretativa que hay que tener en cuenta a la hora de analizar el tratamiento de datos de carácter personal con fines policiales[2457]. En alguna de sus sentencias, a pesar de referirse específicamente a los supuestos de tratamiento de datos con un fin muy determinado, como es la lucha contra el terrorismo, realiza unas consideraciones que han de ser expuestas.

El Tribunal parte de la idea de que las "sociedades democráticas se encuentran amenazadas en nuestros días por formas muy complejas de espionaje y por el terrorismo, de suerte que el Estado debe ser capaz, para combatir eficazmente estas amenazas, de vigilar en secreto los elementos subversivos que operan en su territorio"[2458]. Sin embargo, más adelante aclara el TEDH que cualquiera "que sea el sistema de vigilancia adoptado, el Tribunal debe convencerse de la existencia de garantías adecuadas y suficientes contra los abusos. Esta apreciación no tiene más que un carácter relativo: depende de todas las circunstancias que envuelven el caso, por ejemplo la naturaleza, la extensión y la duración de las medidas eventuales, las razones requeridas para ordenarlas, las autoridades competentes para autorizarlas, ejecutarlas y controlarlas y el tipo de recursos previstos por el derecho interno"[2459].

Queda claro que este Tribunal exige que el tratamiento de datos de carácter personal se lleve a cabo con todas las garantías posibles. En esta misma línea, el Grupo de Trabajo del artículo 29, a la hora de analizar las medidas que han de rodear a todo tratamiento de datos con fines policiales[2460], interpreta la jurisprudencia del citado tribunal al respecto de la materia que se está tratando. Concluye que las medidas legislativas que en los diferentes estados de la unión se están tomando contra el terrorismo, y que afectan a la autodeterminación informativa y a la intimidad[2461], tendrán que demostrar que responden a una "exigencia social imperativa". Las medidas simplemente "útiles" o "convenientes" no pueden restringir los derechos y las libertades fundamentales". Recuerda esta institución que las normas que se dirijan a limitar el derecho que aquí se está analizando deberán ser "accesibles y previsibles en cuanto a sus consecuencias para las personas afectadas. A tal efecto, la legislación ha de ser suficientemente clara en su definición de las circunstancias, el ámbito y las modalidades del ejercicio de las medidas de

presuntos culpables, asegurar los instrumentos, efectos y pruebas del delito, poniéndolos a disposición del juez o tribunal competente y elaborar los informes técnicos y periciales procedentes
h) Captar, recibir y analizar cuantos datos tengan interés para el orden y la Seguridad Pública, y estudiar, planificar y ejecutar los métodos y técnicas de prevención de la delincuencia".

[2457] GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 159, también subraya la importancia de esta jurisprudencia.

[2458] STEDH 6 septiembre de 1978, Caso Klass y otros v. Alemania, FJ 48.

[2459] STEDH 6 septiembre de 1978, Caso Klass y otros v. Alemania,FJ 50.

[2460] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 10/2001, relativo a la Necesidad de un Enfoque Equilibrado en la Lucha contra el Terrorismo, adoptado el 14 de diciembre de 2001.

[2461] Se podría citar en el ámbito interno la aprobación de la Ley 25/2007, de 18 de octubre de 2007, de conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, que en la Exposición de Motivos explica el motivo último de la aprobación de esta norma que es mera transposición de la Directiva 2002/58/CE, de 12 de julio. Se trata de imponer la obligación a los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de que dispongan de ellos los agentes facultados, que no son otros sino los Cuerpos Policiales y el Centro Nacional de Inteligencia. Al respecto, CUBERO MARCOS, y ABERASTURI GORRIÑO, "Protección de datos…", cit., 2008.

interferencia. Las disposiciones deben de ser claras e indicar de forma pormenorizada en qué circunstancias las autoridades públicas están autorizadas para adoptar medidas que limitan derechos fundamentales. Concretamente deben especificar dónde pueden aplicarse tales medidas, excluir toda vigilancia general o preliminar y ofrecer protección contra los ataques arbitrarios de las autoridades públicas". Teniendo en cuenta las consideraciones que se acaban de realizar, hay que analizar ahora si efectivamente es necesario recabar el consentimiento del titular para comunicar sus datos sanitarios a las Fuerzas y Cuerpos de Seguridad.

I.5.4.E.b. El artículo 22.3 LOPD como fundamento de la excepción al consentimiento en la cesión de datos sanitarios a las Fuerzas y Cuerpos de Seguridad.

La regulación de los ficheros policiales en la Ley ha sido especialmente criticada por la doctrina[2462]. Con respecto al contenido del artículo que ahora se analiza, se plantean diferentes cuestiones. El estudio del artículo 22.3 de la LOPD ha de empezar con una consideración crítica a la propia existencia del precepto, que debe llevar a la cautela a la hora de interpretar su contenido.

Desde un punto de vista puramente sustantivo, la disposición que se estudia parte de la idea de que es necesario manipular datos relativos a la orientación religiosa, política, sindical de las personas, así como datos concernientes a la salud, vida sexual o raza de los individuos. Estando de acuerdo en que en determinadas circunstancias este tratamiento será necesario para los fines que se pretenden, no hay que dejar de llamar la atención sobre una cuestión. La posibilidad de investigar a personas basándose en aspectos ideológicos, raciales o sexuales, puede llevar fácilmente a situaciones de discriminación de determinados sectores de la población[2463]. El que el mero hecho de pertenecer a una raza, o de padecer una enfermedad, o tener una ideología determinada, pueda llevar a un ciudadano a ser investigado tiene que repugnar a una democracia que se considera consolidada, más aún cuando la CE dispone que "*nadie podrá ser obligado a declarar sobre su ideología, religión o creencias*"[2464]. La posibilidad de crear ficheros de datos de personas relacionadas entre sí exclusivamente por razón de su orientación sexual, raza o ideología, ha de considerarse como una alternativa *a priori* rechazable. Desde el Consejo de Europa ya con prontitud se puso de manifiesto que este tipo de ficheros sólo pueden crearse en situaciones excepcionales[2465]. El empleo de este tipo de informaciones incluso con los fines

[2462] HERRÁN ORTIZ, *El Derecho…,* cit., 2002, p. 276; MARTÍNEZ MARTÍNEZ, "Ficheros Policiales…", cit., 2005.
[2463] TORNE-DOMBIDAU JIMÉNEZ y CASTILLO BLANCO, "Informática y... (II)", cit., 1993, p. 286, consideran que "la utilización de datos ultrasensibles, las excepciones en ciertos casos, etc... se basan en determinadas presunciones de que ciertas religiones, ideologías o tendencias sexuales son proclives al delito, olvidando que <<el pensamiento no delinque>> que los comportamientos sexuales no generan delitos, ni los datos relativos a la salud, ni los religiosos etc...". "Sin embargo, la realización de dichas presunciones (...) podrían ser discriminatorias para ciertos colectivos al estar basadas en hechos no necesaria ni universalmente ciertos".
[2464] Artículo 16.2 CE.
[2465] Artículo 2.4 Recomendación 15 (1987), de 17 de septiembre de 1987. del Consejo de Europa, que regula el uso de los datos de carácter personal en el sector de la policía: "*The Collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried aout if absolutely necessary for the purpouses of a particular inquiry*".

que se recogen en el artículo comentado tiene que estar limitado a unos supuestos muy bien determinados[2466] y siempre tiene que llevarse a cabo con las máximas garantías[2467].

Partiendo de esta consideración, la aplicación del artículo 22.3 LOPD en el ámbito sanitario plantea diferentes dudas. A) En primer lugar, el que dicho precepto no haga ninguna referencia a la cesión crea la incertidumbre de si es aplicable a este tipo de operaciones[2468]. La Ley dispone que los datos especialmente protegidos pueden ser "recogidos y tratados" cuando dichas acciones sean absolutamente necesarias para la realización de una investigación concreta[2469]. Cabe preguntarse si la cesión de los datos sanitarios con los fines comentados tiene cabida en el ámbito de aplicación de este precepto de la norma.

No hay que forzar demasiado la letra de la Ley para dar una respuesta afirmativa[2470]. Si la norma se aplica tanto al tratamiento como a la recogida, parece que las transmisiones han de tener cabida en este punto. La recogida de datos, como ya se ha apuntado anteriormente, puede referirse tanto a la recogida originaria de los datos del propio titular, como a una recogida llevada a cabo tomando como fuente a un tercero. Esta última podría consistir en una cesión de datos. En este caso, el centro sanitario comunicaría datos relativos a la salud a los cuerpos y fuerzas de seguridad. También podría interpretarse el concepto de tratamiento en un sentido amplio, incluyendo la cesión dentro de su ámbito de aplicación. En todo caso, parece que no hay problema para que la regulación del artículo 22.3 LOPD, concerniente al tratamiento por las Fuerzas y Cuerpos de Seguridad de datos que requieren una especial protección, sea aplicable a la cesión de estos datos. Lo cierto es que la falta de aplicación de este precepto a las cesiones generaría una laguna jurídica de negativas consecuencias, pues dejaría sin regulación la operación que ahora se analiza.

B) En segundo lugar, se plantea la duda de si cabe la excepción del consentimiento para realizar la cesión de los datos sanitarios en estos casos. Se reconoce en el artículo 22.2 de la Ley la posibilidad de tratar los datos de carácter personal, en general, con la finalidad de salvaguardar la seguridad pública y de reprimir las infracciones penales, sin necesidad de recabar el consentimiento del titular de los datos. Aquí se recoge expresamente la posibilidad de tratar este tipo de datos, se podrían llamar comunes, sin el consentimiento del titular. Más allá de la indeterminación de los términos que se emplean en el precepto, parece lógico que para el cumplimiento de finalidades tan relevantes como las que se citan, el requerimiento del consentimiento se vea exceptuado. Lo contrario obstaculizaría, indudablemente, el cumplimiento de dichos objetivos. Otorgar a los particulares titulares de los citados datos la posibilidad de hacer inviable una investigación policial, oponiéndose a su tratamiento, parece poco afortunado.

Al contrario de lo que sucede en el precepto que se acaba de citar, en la regulación de los datos especialmente protegidos por la Ley, en el artículo 22.3, no se hace expresa referencia a la

[2466] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...*, cit., 2001, p. 168: "la regla general es la prohibición; sólo si no hay más remedio debería admitirse muy excepcionalmente esta práctica".
[2467] MARTÍN PALLÍN, "Tratamiento de ...", cit., 1999, p. 115.
[2468] GUICHOT, *Datos Personales…,* cit., 2005, p. 429.
[2469] Artículo 22.3 LOPD.
[2470] TRONCOSO REIGADA, *Protección de datos…,* cit, 2008, p. 101.

falta de necesidad del consentimiento del titular cuando la información es manipulada con los citados fines. En este caso, simplemente se señala que estos datos, los relativos a la salud entre ellos, podrán ser empleados con la finalidad de llevar a cabo una investigación. El precepto no recoge esa limitación, es decir, no dispone expresamente que no es preciso el consentimiento para el tratamiento de datos. De este modo, teniendo en cuenta que la limitación de un derecho fundamental debe estar expresamente prevista en la Ley, podría entenderse que para el tratamiento de los datos sanitarios por las Fuerzas y Cuerpos de Seguridad hay que recabar el consentimiento expreso de los afectados[2471]. Cabe preguntarse si es posible aceptar el criterio contrario al expuesto y admitir también aquí una excepción al consentimiento[2472].

A pesar de que el artículo 22.3 LOPD no lo apunte expresamente, no está claro que para tratar la información especialmente protegida en la Ley con fines de investigación policial sea necesario el consentimiento del titular y, en la práctica, parece asumido que en la voluntad del legislador está la posibilidad de que estos datos puedan ser manipulados sin el consentimiento de los titulares[2473]. Haciendo un ejercicio de ponderación entre diferentes bienes jurídicos, no parece descabellado afirmar que los datos denominados sensibles pueden ser tratados sin la autorización de su titular cuando el fin es tan relevante como la prevención de delitos. La fórmula que se recoge en el artículo 22.2 de la Ley puede resultar perfectamente aplicable, siempre que se establezcan las garantías necesarias, para los datos especialmente protegidos.

Las diferentes instituciones que dirigen su actividad a asegurar el cumplimiento de las normas que regulan la protección de datos no han concretado el contenido del precepto que aquí se analiza. Tampoco la jurisprudencia se ha pronunciado en muchas ocasiones sobre este punto. No obstante, en los escasos supuestos en los que lo ha hecho parece dar a entender, pues tampoco lo afirma expresamente, que el régimen jurídico aplicado al consentimiento es el mismo tanto en el artículo 22.2 como en el 22.3 de la Ley[2474].

C) Si se concluye que la Ley admite definitivamente la posibilidad de manipular los datos relativos a la salud de las personas, con la finalidad de llevar a cabo investigaciones de carácter policial, sin el consentimiento del titular, parece fundamental aclarar cuál es el ámbito de aplicación de dicha excepción al consentimiento. Hay que tener en cuenta que se está haciendo referencia a limitar una de las facultades más relevantes que completan el derecho fundamental a la autodeterminación informativa. Esta consideración lleva a que se hayan de tomar todas las cautelas necesarias a la hora de definir dicha excepción. En este sentido, el Consejo de Europa, en la Recomendación sobre el uso de datos de carácter personal en el ámbito policial ha

[2471] OROZCO PARDO, "La Protección...", cit., 2002, p. 233, lo ha entendido así cuando afirma que "el 22.3 no permite tratar sin consentimiento los datos del art. 7.2 y 3 pues no lo dice expresamente".
[2472] MURILLO DE LA CUEVA, *Informática y Protección...*, cit., 1993, p. 108. "¿La ley contempla como un todo, como un *continuum* los supuestos de ambos párrafos de manera que el enunciado del primero que permite proceder sin el consentimiento debe considerarse subsistente en el segundo? Tal vez sea esa la intención que motivó al legislador, pero no resulta con claridad de la ley. Entonces, ¿ha de interpretarse en contra de los derechos fundamentales? Ciertamente no. Si, pese a todo, se procediera de ese modo *contra libertatis*, habría que sostener la tacha de inconstitucionalidad frente a dicha interpretación".
[2473] FERNÁNDEZ GARCÍA, "Ficheros de las Fuerzas…", cit., 2008, pp. 443-444.
[2474] STS 20 de mayo de 2008, FJ 4.

dispuesto expresamente, que el fin policial no puede suponer en ningún caso la justificación de una recogida y tratamiento de datos indiscriminado[2475].

Por un lado, a pesar de que no se requiera el consentimiento del titular, los principios de calidad antes analizados deben guiar en todo caso el tratamiento de los datos de carácter personal. Si bien es indudable que la finalidad guarda en este caso una relevancia especial, los datos que se manipulan tienen que ser los estrictamente necesarios para el cumplimiento del fin policial determinado, los imprescindibles para llevar a cabo la investigación pertinente. Cierto es que el Convenio 108/1981 exceptúa la aplicación de los principios de calidad cuando la finalidad es la represión de una infracción penal[2476]. A pesar de ello, la citada memoria explicativa de la Recomendación del Consejo de Europa sobre la protección de datos médicos parece reconocer que el principio de pertinencia deberá ser atendido en todo caso. Lo contrario supondría la anulación o suspensión del derecho a la autodeterminación informativa en este ámbito. Ciertamente, no parece que puedan establecerse excepciones como la que se acaba de plantear a los principios recogidos en el artículo 4 de la LOPD, pues, como se dijo en el capítulo anterior, estos principios reconocen las garantías mínimas que todo tratamiento de datos ha de cumplir[2477].

El precepto que se analiza dispone que el tratamiento de estos datos sólo se dará cuando sea "absolutamente necesario" para llevar a cabo una investigación. El legislador es consciente de la necesidad de restringir la aplicación del límite que se plantea al derecho fundamental a la autodeterminación informativa a supuestos muy concretos. Como se dijera al analizar el artículo 24 de la Ley, se trata de la estricta aplicación del principio de proporcionalidad.

Por otro, la excepción al consentimiento se dará cuando los datos relativos a la salud se manipulen con el fin de realizar "una investigación concreta". De inicio, la cesión podrá darse siempre que exista una investigación. No parece que pueda admitirse esta operación en relación

[2475] Recomendación 15 (1987), 17 de septiembre de 1987, que regula el Uso de los Datos Personales en el Ámbito Policial.

[2476] Artículo 9.2.a) Convenio 108/1981 del Consejo de Europa: *"será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio* (el artículo 5 recoge los principios de calidad) *cuando tal excepción, prevista por la Ley de la Parte, constituya una medida necesaria en una sociedad democrática: para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales"* (el subrayado es nuestro).

[2477] Punto 78 Memoria Explicativa Recomendación R (97) 5 del Consejo de Europa: "*The drafters of the recommendation agreed that medical data could furthermore be collected without consent, if provided for by law, for the prevention of a real danger or the suppression of a specific criminal offence. Rather than the terminology used in Article 9 of the convention, they preferred the wording used in Recommendation Nº R(87) 15 regulating the use of personal data in the police sector. Principle 2.1 of this recommendation excludes an open-ended, indiscriminate collection of data by the police. It expresses a qualitative and quantitative approach to Article 5.c of the convention which stipulates that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are stored. Given that article 9.a of the convention allows a derogation from this principle in regard to the "suppression of criminal offences", principle 2.1 of the recommendation attempts to fix the boundaries to this exception by limiting the collection of personal data to such as are necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless domestic law clearly authorises wider police powers to gather information. "Real danger" is to be understood as not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities. (...)".*

a los datos sanitarios cuando la investigación no haya tenido comienzo[2478]. Sin embargo, ¿a qué tipo de investigación se refiere la norma? Se ha planteado la posibilidad de realizar una interpretación especialmente restrictiva del precepto, entendiendo que se refiere únicamente a la investigación o persecución de un delito ya cometido[2479]. Quedaría fuera de este concepto, por ejemplo, la actividad policial preventiva.

Frente a esta interpretación también es posible un criterio más amplio. El artículo 22.3 sólo se refiere al empleo de la información con el fin de llevar a cabo una "investigación concreta". Una investigación puede darse bien para reprimir un delito que ya se ha producido, o para prevenir que se produzca. En este sentido, el contenido del concepto "investigación concreta" podría determinarse haciendo un paralelismo con el artículo 22.2 de la Ley. Esta disposición apunta a la "prevención de un peligro real para la seguridad pública o para la represión de infracciones penales". Se englobarían aquí actividades tanto represivas como preventivas[2480]. Se podría entender que este contenido es trasladable al artículo 22.3 de la Ley. La interpretación del concepto "represión de infracciones penales" no presenta mayores problemas. No obstante, hay que subrayar la necesidad apuntada por la jurisprudencia de que se trate de la investigación de un ilícito penal, no administrativo[2481]. Por el contrario el concepto de "prevención de un peligro real para la seguridad pública", puede abrir las puertas a diferentes y múltiples supuestos, como se vio al analizar el artículo 24.1 de la Ley. En ese momento se puso de manifiesto la falta de concreción del concepto de seguridad pública[2482]. La misma indeterminación resulta de la referencia a la existencia de un peligro real[2483]. No es sencillo aclarar cuándo se produce esta circunstancia. La normativa sobre las Fuerzas y Cuerpos de Seguridad no ayuda a aclarar estos términos. La memoria explicativa de la Recomendación del Consejo de Europa sobre la protección de los datos médicos otorga un sentido amplio al concepto de "prevención de peligro real", excluyendo solamente los casos de sospecha infundada de existencia de delito o de posible comisión de delito[2484].

A falta de mayores referencias, se puede concluir que la redacción de las normas abre un amplio campo de actuación para las Fuerzas y Cuerpos de Seguridad. En todo caso, no hay que olvidar que, cuando se trata de datos que requieren de especial protección las cesiones sólo podrán llevarse a cabo sin el consentimiento del interesado cuando sean absolutamente necesarias para cumplir los citados fines. De esta manera, el ámbito de aplicación de la excepción se restringe.

[2478] ZAMORA JIMÉNEZ, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.420.
[2479] CASADO CADARSO y VILA MUNTAL, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.400.
[2480] ZAMORA JIMÉNEZ, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.415.
[2481] SAN 8 de junio de 2001, FJ 5.
[2482] CASADO CADARSO y VILA MUNTAL, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.398; ZAMORA JIMÉNEZ, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.420.
[2483] CASADO CADARSO y VILA MUNTAL, "Los ficheros de las Fuerzas…", cit., 2010, p. 1.398.
[2484] Señala el Consejo de Europa, en el punto 78 de la Memoria Explicativa Recomendación R (97) 5 del Consejo de Europa, que hay que entender por "peligro real", no una infracción o infractor determinado, sino cualquier circunstancia que genere una sospecha razonable sobre la producción de una infracción penal, excluyendo toda especulación infundada.

Por último, la crítica principal al precepto que ahora se analiza es la falta de previsión por parte de la norma de garantía alguna dirigida a evitar la arbitrariedad en la actuación de las policías a la hora de acceder a información sanitaria[2485]. De inicio, podría pensarse que estos órganos pueden actuar en cualquier momento, en base a su propio criterio, para cumplir las funciones que tienen asignadas. Hay que tener en cuenta que la ambigüedad de los conceptos empleados en el precepto analizado favorece la discrecionalidad en su aplicación. Esta posibilidad generaría una gran incertidumbre o inseguridad para los ciudadanos, que podrían ver cómo se accede a sus datos sanitarios sin control. Con el fin de limitar esta discrecionalidad, el artículo comentado, empleando una redacción poco clara, dispone que es necesario un "*control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales*". Se establece, por lo tanto, un sistema de fiscalización de la actuación de las Fuerzas y Cuerpos de Seguridad. Sin embargo, de una primera lectura de este texto no es fácil saber a qué tipo de control se refiere este precepto. En un inicio parece que se limita a un control *a posteriori* de la actuación policial llevado a cabo por los órganos jurisdiccionales. Siendo así, el control se produciría una vez se hubiera causado un daño a los titulares de los datos. Esta medida es insuficiente y hubiera sido recomendable fijar como requisito para llevar a cabo el acceso comentado un control previo. En esta línea, se está de acuerdo con quienes abogan por admitir la necesidad de recabar una previa autorización judicial para realizar estas operaciones[2486].

Como se ha visto, el requerimiento de la intervención previa de la autoridad judicial no queda claro en el ordenamiento para estos casos. En relación al artículo 22.2 de la LOPD la AEPD ha dado a entender que es suficiente con la habilitación legal para que la policía judicial pueda acceder a la información que estime oportuna[2487]. No obstante, haciendo una interpretación sistemática del ordenamiento, no resulta descabellado plantear la necesidad de autorización judicial previa para que las Fuerzas y Cuerpos de Seguridad puedan acceder a los datos sanitarios.

Ya se planteó en la tramitación parlamentaria de la LOPD por el Grupo Parlamentario Vasco[2488], que ha de ser una autoridad judicial la que determine, en cada caso, cuándo se dan las circunstancias que justifican la cesión de la información sanitaria en estos supuestos. En primer lugar, hay que tener en cuenta que la falta de la intervención judicial previa dejaría a los profesionales sanitarios en la tesitura de tener que interpretar en cada momento si la ruptura de la obligación de secreto que van a llevar a cabo con la ejecución de la cesión está o no justificada[2489].

En segundo lugar, la necesidad de que sea la autoridad judicial quien autorice la intrusión en el derecho fundamental al derecho a la autodeterminación informativa puede encontrar base en

[2485] GARRIGA DOMÍNGUEZ, *La Protección...*, cit., 1999, p. 214, sostiene la inconstitucionalidad del precepto comentado.
[2486] HERRÁN ORTIZ, *El derecho a la intimidad…,* cit., 2002, p. 277.
[2487] Informe jurídico de la AEPD, 0133/2008.
[2488] Enmienda nº 32 del Grupo Parlamentario Vasco (EAJ-PNV), BOCG nº 135-7, 4 de noviembre de 1998,
[2489] TRONCOSO REIGADA, *Protección de datos...,* cit, 2008, p. 101; HERRÁN ORTIZ, *El Derecho…,* cit., 2002, p. 277.

diferentes textos normativos. Primero, la propia Constitución reclama dicha autorización para otras vulneraciones del derecho a la intimidad, como puede ser la violación de la intimidad domiciliaria o la violación del secreto de las comunicaciones[2490]. Segundo, en esta misma línea, el ordenamiento ha reconocido para el supuesto en que los agentes policiales quieren acceder a bases de datos de carácter personal en manos de los operadores de telecomunicaciones, que además contienen información que no pertenece al grupo de datos que requieren una especial protección, la necesidad de recabar la previa autorización judicial[2491]. La jurisprudencia ha señalado que en estos casos la exigencia de la autorización judicial viene motivada porque más allá del derecho a la protección de datos se ve afectado también el secreto de comunicaciones[2492]. El que puedan verse vulnerados diferentes bienes jurídicos de especial relevancia hace que se deban adoptar las máximas garantías posibles. Siguiendo esta línea interpretativa se podría afirmar que en el caso en que las Fuerzas y Cuerpos de Seguridad quieren acceder a datos sanitarios ocurre algo parecido. En este supuesto dicho acceso no sólo afecta a la autodeterminación informativa de los pacientes, sino que también al secreto profesional, recogido como garantía constitucional en el artículo 24.2 CE. Esta circunstancia vendría a justificar sobradamente la necesidad de requerir autorización judicial para poder llevar a cabo el acceso a la información.

De todo lo expuesto cabe concluir que en este punto la letra de la Ley presenta grandes lagunas y es especialmente criticable, por un lado, debido a la ambigüedad de los términos que emplea y al hecho de que no se pronuncia expresamente sobre la posibilidad de exceptuar el derecho a consentir y, por otro, porque no aclara las garantías que han de respetarse a la hora de que las policías accedan a los datos de carácter personal. A pesar de ello ha sido posible realizar una interpretación sistemática de la LOPD y de otras normas, ajustando el marco en el que se realizan esos tratamientos de datos a criterios más protectores del derecho a la autodeterminación informativa. De esta forma, aunque se entiende que el acceso de las Fuerzas y Cuerpos de Seguridad a los datos sanitarios es posible sin necesidad de recabar el consentimiento de su titular para el cumplimiento de una serie de funciones, esta manipulación deberá cumplir con los requisitos que se han expuesto en este apartado.

[2490] Artículo 18 CE; Artículo único de la LO 2/2002, 6 de mayo, reguladora del Control Judicial previo del Centro Nacional de Inteligencia: "*El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro (...)*".

[2491] Artículo 7, Ley 25/2007, de 18 de octubre de 2007, de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones: "*1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.*
2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados (...)". STS 18 de marzo de 2010, FJ 3. MORENO CATENA, "Ley de Conservación…", cit., 2008, p. 170.

[2492] STS 20 de mayo de 2008, FJ 4.

I.5.4.F. Colisión entre el deber de secreto médico y la obligación de colaborar con la justicia.

I.5.4.F.a. Cuestiones previas.

La LOPD dispone que no se requiere el consentimiento del titular para llevar a cabo la cesión de los datos de carácter personal cuando los destinatarios sean el Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, siempre que se encuentren en el ejercicio de las funciones que legalmente tienen atribuidas. Lo mismo ocurre cuando la comunicación de datos se dé a favor de figuras análogas al Defensor del Pueblo o Tribunal de Cuentas en el ámbito autonómico[2493]. El reglamento que desarrolla la Ley reproduce en los mismos términos esta excepción[2494]. Por su parte, la memoria explicativa de la Recomendación del Consejo de Europa sobre protección de datos médicos reconoce, que los datos podrán ser cedidos cuando la comunicación sea necesaria para probar, ejercer o defender un derecho ante a un juez o tribunal[2495].

En la normativa sanitaria la excepción al consentimiento que se comenta se recoge en un sentido parecido al citado. La LBAP reconoce la posibilidad de acceder a una historia clínica con fines judiciales. Dispone que no es necesario el consentimiento del titular, para que jueces y tribunales accedan a los datos sanitarios con el fin de llevar a cabo la investigación judicial pertinente[2496]. En el ámbito autonómico las citas han sido muy parecidas[2497]. En la normativa sanitaria las cesiones tienen como destinatarios los órganos judiciales. No se encuentran referencias expresas a las demás instituciones que en la normativa de protección de datos tenían cabida: Defensor del Pueblo, Tribunal de Cuentas, etc. A pesar de ello, no parece que haya dificultad para extender esta excepción a los otros sujetos indicados en la LOPD. Primero, porque es necesario realizar una interpretación conjunta de todas las normas aplicables para concluir en qué supuestos se exceptúa el consentimiento en la cesión de datos sanitarios. Y segundo, porque es incuestionable que estos organismos dirigen gran parte de su actividad a la defensa y

[2493] Artículo 11.2.d) LOPD.
[2494] Artículo 10.4.b) RDLOPD.
[2495] Punto 148 Memoria Explicativa de la Recomendación R (97) 5 del Consejo de Europa: "*secondly, medical data may be communicated if such communication is necessary for the proof, exercise or defence of a right in court. As this concerns communication of sensitive data, in the interest of a third person, without the knowledge of the data subject and for purpouses incompatible with those of collection, the drafters of the recommndation emphasised that the proof, exercise or defence of a right in court shall prevail over the right to privacy of the data subject"*.
[2496] Artículo 16.3 LBAP. "*El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en la Ley 14/1986, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos. Se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínico-asistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso*".
[2497] Artículo 13 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el Uso y Acceso a la Historia Clínica electrónica: *"Se establece la plena colaboración con la Administración de Justicia, de modo que el sistema IANUS facilitará siempre el acceso a la información contenida en la historia clínica electrónica del/de la paciente o usuario/a para la investigación judicial. Cuando la autoridad judicial lo considere imprescindible y así lo solicite, se facilitará la información completa de la historia clínica electrónica con la unificación de los datos identificativos y los clínico-asistenciales. En el resto de los supuestos, la información quedará limitada estrictamente para los fines específicos de cada caso*".

promoción de los derechos fundamentales[2498]. Ya se vio en apartados anteriores la posibilidad de que, por ejemplo, el Defensor del Pueblo acceda a los datos sanitarios para desarrollar sus funciones. En cualquier caso, lo que ahora interesa es el caso concreto de la cesión de los datos sanitarios a favor de Jueces y Tribunales.

De las indicaciones que se han dado parece deducirse que las cesiones de datos sanitarios a las autoridades judiciales para el adecuado ejercicio de sus funciones no requerirán del consentimiento de su titular[2499]. No se establece mayor matiz, por lo que podía resultar un límite absoluto a dicho derecho. En este mismo sentido, la jurisprudencia ha reconocido en ocasiones la necesidad de recabar la mayor información posible para el desarrollo de sus investigaciones, reforzando esta posibilidad de ceder datos, incluso sanitarios, a favor de los órganos judiciales[2500]. En la práctica es constante el empleo de la historia clínica como prueba en los procesos judiciales dirigidos a aclarar supuestos de responsabilidad médica[2501].

Si bien este punto de partida no parece plantear ningún problema interpretativo, lo cierto es que estas cesiones de datos generan mayores dudas de las que puedan resultar de una primera lectura de las normas. La excepción que se está analizando genera un conflicto de intereses de especial envergadura que no tiene fácil solución[2502]. Se trata fundamentalmente del enfrentamiento entre la obligación de guardar o respetar el secreto profesional por parte de los profesionales sanitarios y la obligación de éstos de colaborar con la justicia. Es conocida la relevancia que puede tener la historia clínica como medio de prueba en los más diversos procesos judiciales[2503]. Esta circunstancia se ha puesto de manifiesto también por la jurisprudencia[2504].

Entran en juego aquí diferentes bienes jurídicos. Por un lado se encuentra la obligación reconocida en la propia CE[2505] y en la LOPD[2506] de respetar el secreto profesional. La Ley de Enjuiciamiento Criminal recoge también la vigencia del secreto para los procesos penales[2507]. Así lo hace, a su vez, la Ley de Enjuiciamiento Civil[2508]. Basándose en este deber de secreto, el

[2498] TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 85.
[2499] GÓMEZ PIQUERAS, "La historia clínica…", cit., 2009, p. 152.
[2500] STC 2 de marzo de 1989, FJ 4, en la que se justifica la entrada y registro por orden judicial en una clínica para acceder a determinados datos sanitarios de una persona implicada en un proceso judicial; STS 2 de diciembre de 1996, FJ 1; SAN 26 de noviembre de 2008, FFJJ 3 y 4; STEDH 25 febrero de 1997, Z vs. Finlandia, FJ 97 y siguientes.
[2501] SSTS 25 de abril de 2005, FFJJ 4 y 5; 14 de febrero de 2006, FJ 6; 23 de noviembre de 2007, FJ 2.
[2502] CANTERO RIVAS, "La Historia…", cit., 2004, pp. 340-341.
[2503] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 545
[2504] SAP Barcelona 5 de enero de 1998, FJ 1; SAN 11 de enero de 2010, FJ 4, en el que se decide que los datos de salud de una persona han de ser trasladados a sede judicial en la medida en que constituyen elemento relevante de prueba.
[2505] Artículo 24.2 CE, segundo párrafo: "*La Ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos".*
[2506] Artículo 10 LOPD.
[2507] Artículo 417.2 LECrim: *"No podrán ser obligados a declarar como testigos: Los funcionarios públicos, tanto civiles como militares, de cualquier clase que sean, cuando no pudieren declarar sin violar el secreto que por razón de sus cargos estuviesen obligados a guardar, o cuando, procediendo en virtud de obediencia debida, no fueren autorizados por su superior jerárquico para prestar la declaración que se les pida".*
[2508] Artículo 371.1 LEC: *"Cuando, por su estado o profesión, el testigo tenga el deber de guardar secreto respecto de hechos por los que se le interrogue, lo manifestará razonadamente y el tribunal, considerando el fundamento de la*

profesional no estaría obligado a transmitir la información de sus pacientes a los jueces. Puede defenderse esta posición basándose en otro principio. Concretamente, podría argumentarse el derecho a no declarar contra sí mismo o autoinculparse como fundamento de la negativa a trasladar la información sanitaria a un proceso judicial[2509]. Piénsese, por ejemplo, en el caso del médico que no quiere ceder la Historia Clínica a un proceso determinado pues entiende que contiene información que podría perjudicarle.

A estos derechos se les oponen otros reconocidos en la misma Constitución, como el de tutela judicial efectiva[2510]. Este último obliga a actuar en los procesos judiciales con la máxima información posible, siempre que sea pertinente[2511], lo que podría llevar a exigir que los profesionales sanitarios tuvieran que romper su obligación de guardar silencio y transmitir determinados datos de sus pacientes. Podría alegarse también, a favor de la necesidad de aportar datos de carácter personal sanitarios a un proceso judicial determinado, la obligación que la CE establece de colaborar, en todo caso, con los jueces y tribunales[2512]. La LOPJ también recoge esta obligación[2513]. La falta de esta colaboración atenta contra las reglas de buena fe que deben respetarse en todo tipo de procedimientos[2514].

Como se ha subrayado, el secreto profesional se erige en una institución de particular relevancia en el ámbito sanitario. Sin embargo, no se puede negar que la información relativa a un paciente puede ser de vital importancia en un determinado proceso judicial para que la resolución que se adopte esté lo más fundamentada posible. Hay que tratar por lo tanto de buscar el equilibrio entre los bienes jurídicos en juego.

La LOPD y las demás normas que se han citado no son demasiado clarificadoras. Las dudas son numerosas y, como se verá, la inseguridad que genera en el ámbito médico el hecho de que no esté claro cómo resolver esta colisión de intereses, hace necesaria una norma que determine cuándo y cómo ha de actuar un profesional sanitario ante el llamamiento de un juez o magistrado para que ceda información sanitaria de un paciente[2515]. A falta de esta norma no cabe otra cosa que llevar a cabo un ejercicio de interpretación para tratar de determinar los criterios que se han de seguir al resolver el conflicto.

---

negativa a declarar, resolverá, mediante providencia, lo que proceda en Derecho. Si el testigo quedare liberado de responder, se hará constar así en el acta".

[2509] Artículo 24.2 CE, párrafo primero: "*Asimismo, todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia".*

[2510] Artículo 24.1 CE: "*Todas las personas tienen derecho a obtener la tutela efectiva de los jueces y tribunales en el ejercicio de sus derechos e intereses legítimos, sin que, en ningún caso, pueda producirse indefensión".*

[2511] STS 4 de diciembre de 2009, FJ 4.

[2512] Artículo 118 CE: "*Es obligado cumplir las sentencias y demás resoluciones firmes de los Jueces y Tribunales, así como prestar la colaboración requerida por éstos en el curso del proceso y en la ejecución de lo resuelto*". OTERO GONZÁLEZ, *Justicia y Secreto…*, cit., 2001, p. 15; COUDERT, "Tratamiento de datos…", cit., 2007, p. 356.

[2513] Artículo 17 LOPJ: "*Todas las personas y entidades públicas y privadas están obligadas a prestar, en la forma que la Ley establezca, la colaboración requerida por los Jueces y Tribunales en el curso del proceso y en la ejecución de lo resuelto, con las excepciones que establezcan la Constitución y las Leyes, y sin perjuicio del resarcimiento de los gastos y del abono de las remuneraciones debidas que procedan conforme a la Ley*".

[2514] STS 15 de noviembre de 1991, FJ 4.

[2515] SAP de Guipuzcoa 29 de noviembre de 2004.

I.5.4.F.b. La no inculpación y el derecho a la tutela judicial efectiva: una difícil relación.

En primer lugar, cabe analizar el enfrentamiento entre el derecho a no autoinculparse en el transcurso de un procedimiento sancionador contra los médicos, pacientes o terceros, y la obligación de transmitir información relativa a un proceso sanitario determinado cuando así lo requiere un juez o magistrado. No se hará en este momento un análisis en profundidad sobre la definición y contenido del derecho a no autoinculparse[2516]. Basta para los fines que aquí se pretenden con una aproximación al contenido de este derecho.

La Constitución reconoce expresamente el derecho a no declarar contra sí mismo y a no confesarse culpable[2517]. Así lo hace también el Pacto Internacional de Derechos Civiles y Políticos[2518]. El Convenio Europeo de Derechos Humanos, según ha señalado el TEDH, integra este derecho en el más amplio derecho a un proceso justo[2519].

Según la jurisprudencia, la autoinculpación supone emitir una declaración de voluntad que exteriorice la admisión de la culpabilidad de uno[2520]. El derecho a no autoinculparse, por lo tanto, consiste en la facultad de no emitir una tal declaración admitiendo la culpabilidad en un procedimiento sancionador. Así, este derecho se vulnera cuando se exige, obliga o compele a una persona a que lleve a cabo la citada declaración[2521]. El derecho a no autoinculparse se erige en un medio de protección contra cualquier tipo de coerción ilegítima que pueda condicionar la voluntad de un sujeto a la hora de pronunciarse sobre su culpabilidad con respecto a unos hechos[2522]. La relevancia de este derecho es manifiesta. Constituye, por un lado, un instrumento necesario para hacer efectivo el más genérico derecho a defenderse. Cada uno tiene la facultad de defenderse como crea conveniente, incluso con el silencio o la pasividad[2523], o la mentira[2524]. Por otro lado, se trata de un derecho vinculado directamente con la presunción de inocencia. La facultad de no declararse culpable hace que recaiga en quien acusa la obligación de probar la culpabilidad del acusado[2525].

El derecho a no autoinculparse podría ser entendido, tal como se ha hecho por la doctrina, como un límite al deber de colaborar con los tribunales[2526]. Esta facultad puede ser interpretada en un sentido expansivo. Normalmente cuando se hace referencia a la autoinculpación se está pensando solamente en la confesión. Evidentemente, esta será la forma más común de autoinculparse. Sin embargo, no sería descabellado argumentar que este derecho no sólo abraza

[2516] PALAO TABOADA, *El Derecho…,* cit., 2008.
[2517] Artículo 24.2 CE.
[2518] Artículo 14.3.g) Pacto Internacional de Derechos Civiles y Políticos, 16 de diciembre de 1966.
[2519] Artículo 6 CEDH. STEDH 8 de febrero de 1996, John Murray v. Reino Unido, apartados 45, 46 y 47. ESPARZA LEIBAR y ETXEBARRIA GURIDI, "Comentario al artículo 6…", cit., 2009, p. 242.
[2520] STC 2 de octubre de 1997, FJ 7.
[2521] MONTAÑÉS PARDO, *La Presunción…,* cit., 1999, p. 136.
[2522] SSTS 31 de mayo de 2007, FJ 57; 25 de mayo de 2010, FJ 2. STC 17 de noviembre de 2008, FJ 6.
[2523] SSTC 21 de diciembre de 1995, FJ 6: "Los derechos a no declarar contra sí mismo y a no confesarse culpable (…) son garantías o derechos instrumentales del genérico derecho de defensa, al que prestan cobertura en su manifestación pasiva, esto es, la que se ejerce precisamente con la inactividad del sujeto"; 16 de mayo del 2000, FJ 4. STDEH 2 de mayo del 2000, Condron v. Reino Unido, apartado 56, en el que se pone de manifiesto el valor del silencio.
[2524] STC 7 de julio de 2005, FJ 3.
[2525] STC, 2 de octubre de 1997, FJ. 5. SANZ DÍAZ-PALACIOS, *Derecho a no autoinculparse…,* cit., 2004, p. 54.
[2526] DÍEZ-PICAZO GIMÉNEZ, "Artículo 24…", cit., 2006.

la facultad de no declararse culpable, sino también a no entregar documentos que inequívocamente demuestren la culpabilidad de una persona[2527]. En la medida en que unos documentos incriminan indudablemente a un sujeto unos hechos, podría plantearse que el derecho a no autoinculparse constituye argumento suficiente para no aportar dicha documentación a un proceso judicial determinado.

La autoinculpación, en lo que aquí interesa, podría producirse con la entrega de determinados datos sanitarios al proceso judicial. En algunos casos la revelación de esta información puede suponer una forma de inculpar a un sujeto por unos hechos concretos. El derecho a no autoinculparse podría constituir un argumento para negar esta revelación. Lógicamente, este derecho entraría en colisión con la obligación de colaborar con la justicia y el derecho a la tutela judicial efectiva, que exigen contar con la mayor información posible en los procesos judiciales.

Si bien podría parecer que esta colisión es clara[2528], se entiende aquí que en estos supuestos no se estará ante un verdadero conflicto de intereses. Esto se debe a que no se considera que la revelación de los datos sanitarios suponga, en estos casos, una forma de autoinculparse. La posibilidad de alegar el derecho a no autoinculparse se enfrenta a diferentes argumentos.

A) En primer lugar, desde un punto de vista conceptual, no se puede entender, a priori, que remitir la historia clínica de un paciente, o parte de ella, para la resolución de un proceso suponga declarar contra uno mismo. Como ya se ha dicho por algún autor[2529], esa transmisión implica simplemente un elemento más de prueba[2530]. Por un lado, para que se entienda que hay autoinculpación es necesario que exista una declaración de voluntad de la persona. No parece que pueda hablarse de voluntariedad cuando se trata de documentos creados y custodiados por terceras personas y no por la persona que alega el derecho[2531], como es el caso de la historia clínica, cuya existencia además viene reconocida e incluso impuesta por el ordenamiento. Por otro lado, para que haya dicha autoinculpación es necesario que la documentación que se presenta incrimine al sujeto. No debe bastar con que se trate de materiales que constituyan meros indicios de culpabilidad. La mayoría de veces, los datos sanitarios difícilmente podrán erigirse en argumentos definitivos de incriminación por sí mismos.

Cuando se está ante un proceso sancionador contra un paciente, incluso admitiendo que la historia clínica contenga información que pueda ser considerada como una declaración, el hecho

[2527] STEDH 17 de diciembre de 1996, Saunders v. Reino Unido, apartados 67 y siguientes. ALARCÓN SOTOMAYOR, *El Procedimiento Administrativo…,* cit., 2007, p. 212, hace referencia, aunque en relación a procedimientos administrativos, a la posibilidad de que la entrega de unos documentos suponga una declaración autoincriminatoria.

[2528] OTERO GONZÁLEZ, *Justicia y Secreto…,* cit., 2001, p. 35, reconoce que "cuando la entrega de la historia clínica al juez se produce en un proceso en el que el médico es el inculpado, parece que no está obligado a entregarla en base al derecho fundamental de no declarar contra sí mismo (art. 24.2 CE)".

[2529] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, p. 229.

[2530] CANTERO RIVAS, "La historia clínica…", cit., 2002, p. 225; DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, pp. 204-205; MORENA PÉREZ, "Secreto Médico…", cit., 2000, p. 142; DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 126; RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente…,* cit., 2005, p. 225.

[2531] SANZ DÍAZ-PALACIOS, *Derecho a no autoinculparse…,* cit., 2004, pp. 61-62.

de que el documento sea elaborado por una tercera persona hace que sea difícil, de partida, que la aportación a un proceso judicial de esa historia pueda considerarse como autoinculpación[2532]. Si la autoinculpación constituye una declaración de voluntad realizada por la propia persona que se autoincrimina, no parece que la historia clínica cumpla este requisito, en la medida en que este documento es creado por otras personas.

Cuando se trata de un proceso sancionador contra el profesional sanitario, ocurre lo mismo. Por regla general la historia clínica se elabora por diferentes profesionales y, lo que es más importante, basándose en información referente a un tercero. No se puede, por lo tanto, tampoco en este caso, de inicio, argumentar el derecho a no declarar contra uno mismo para negar la transmisión de información sanitaria a un proceso judicial determinado.

B) En segundo lugar, desde un punto de vista más práctico, lo cierto es que la jurisprudencia ha demostrado que el derecho a no autoinculparse no tiene excesivo recorrido en el ordenamiento. Viene a reflejar esta idea el hecho de que se ha admitido por los órganos judiciales que la obligación de someterse a los controles de alcoholemia no constituye un límite al derecho a no autoinculparse[2533]. Lo mismo ocurre cuando la jurisprudencia analiza la colisión entre la obligación de transmitir datos económicos a la administración tributaria y el derecho a no autoinculparse[2534]. Ciertamente, en estos dos supuestos parece que la aplicabilidad del derecho a no autoinculparse es mayor que en el caso que aquí se plantea, en el que se contraponen la obligación de transmitir determinados datos sanitarios en beneficio de una tutela judicial efectiva.

Desde hace tiempo ha sostenido la jurisprudencia la obligación del médico de remitir la historia clínica a los tribunales cuando se trata de dilucidar casos de responsabilidad médica[2535]. La revelación de la información en estos supuestos se estima necesaria, sin que parezca tener cabida el derecho a no autoinculparse. Es más, en relación a estos casos se va abriendo camino en la jurisprudencia una doctrina según la cual, cuando el profesional sanitario no entregue los datos sanitarios a este tipo de procesos se invertirá, en cierta medida, la carga de prueba, teniendo que ser el médico quien demuestre su inocencia[2536]. Es decir, cuando se discute la responsabilidad del profesional sanitario en un proceso determinado será necesario que dicho profesional remita los datos oportunos para facilitar el desarrollo del proceso. En caso contrario, se entenderá que se invierte la carga de prueba, de forma que deberá ser el profesional quien pruebe su inocencia y no la parte contraria la que demuestre la culpabilidad de aquél. Las consecuencias de no aportar la documentación requerida son, por lo tanto, especialmente gravosas.

[2532] SAP de Valencia, 6 de junio de 2008, FJ 1: "no constituyen declaración autoinculpatoria a estos efectos, los materiales cuya existencia es independiente de la voluntad del obligado tributario, por ejemplo, un documento elaborado por terceras personas, que deje constancia de determinados hechos o actos o que contenga una declaración de voluntad de esas personas".
[2533] STC 4 de octubre de 1985, FJ 3; 18 de diciembre de 1997, FJ 6.
[2534] STC 26 de abril de 1990, FJ 10.
[2535] CRIADO DEL RIO, *Aspectos médico-legales…,* cit., 1999, p. 35. STS 6 de febrero de 2001, FJ 10.
[2536] RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente…*, cit., 2005, p. 223; DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 548. STS 2 de diciembre de 1996, FJ 1: pone de manifiesto que los profesionales sanitarios gozan de una posición procesal especialmente ventajosa, en la medida que cuenta con instrumentos y conocimientos especializados; SSTS, 29 de julio de 1998, FJ 2; 23 de diciembre de 2002, FJ 3.

Ante los argumentos expuestos por los tribunales no parece que se pueda hablar en la práctica de autoinculpación cuando se trata la cesión de datos sanitarios a favor de los órganos judiciales[2537]. Se puede concluir, por lo tanto, que es adecuado partir de la idea de que la obligación de trasladar información sanitaria a un proceso judicial no viola, por regla general, el derecho a no autoinculparse. El que se obligue a un sujeto a trasladar una historia clínica u otros datos sanitarios a un proceso judicial determinado difícilmente constituirá una vulneración de dicho derecho. En todo caso, acogiéndose a la prudencia que ha de inspirar cualquier análisis concerniente a la resolución de un enfrentamiento entre derechos fundamentales, no hay que descartar que una interpretación amplia del derecho a no autoinculparse pueda justificar que un profesional sanitario o un paciente no cedan determinados datos sanitarios a un Tribunal para el desarrollo de un proceso judicial[2538]. Evidentemente, y siguiendo lo dicho hasta ahora, deberá tratarse de un caso claro en que la información sanitaria a transmitir refleje la culpabilidad del sujeto implicado.

I.5.4.F.c. El difícil equilibrio entre el deber de secreto médico, y el derecho fundamental a la tutela judicial efectiva y el deber de colaborar con la justicia.

El deber de colaborar con la justicia, vinculado con el derecho a la tutela judicial efectiva, responde en última instancia a la necesidad de que los procesos judiciales se lleven a cabo con todas las garantías posibles. Evidentemente, el hecho de que se aporte a cada proceso toda la información existente respecto de la causa que se trata constituye una garantía de especial relevancia. Hay que tener en cuenta que la falta de datos a la hora de llevar a cabo cualquier proceso judicial puede conllevar la indefensión de una de las partes[2539]. Si alguien reclama la aportación de los datos sanitarios de una persona para defender su posición en un proceso y dichos datos no son facilitados, evidentemente, su capacidad de defenderse se verá menguada. La indefensión se produce en la medida en que se priva a un ciudadano de contar con todos los medios posibles para apoyar su postura[2540]. Los órganos judiciales están obligados a velar porque en todo proceso las partes cuenten con los mismos medios para defender sus posiciones[2541]. En conclusión, si un juez o un tribunal obstaculiza de alguna manera la posibilidad de que se aporte a un proceso determinado toda la información necesaria para que las partes puedan defender sus posiciones en igualdad de condiciones podría entenderse que, efectivamente, se estará dando un caso de indefensión.

No obstante, a esta obligación de colaborar con la justicia, y en última instancia al derecho a la tutela judicial efectiva, se le opone el derecho a la protección de datos de carácter personal, que en el caso que se analiza aparece protegido por el deber de secreto de los profesionales sanitarios. Se plantea si es posible trasladar los datos sanitarios de una persona a sede judicial sin necesidad de contar con su consentimiento. Normalmente, cuando es el propio paciente el que quiere acceder y aportar su historia clínica al proceso no se plantean mayores problemas, más allá de los casos en que pudiera entrar en juego el ya indicado derecho a no autoinculparse

[2537] CANTERO RIVAS, "El contenido de la historia…", cit., 2004, p. 411.
[2538] DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 203.
[2539] STC 4 de abril de 1984, FJ 1. FIGUERUELO BURRIEZA, *El Derecho…,* cit., 1990, p. 78.
[2540] STC 23 de abril de 1986, FJ 1. CHAMORRO BERNAL, *La Tutela…,* cit., 1994, pp. 112-113.
[2541] STC 27 de marzo de 2007, FJ 2. GARBERÍ LLOBREGAT, *El Derecho…,* cit., 2008, 250.

de un profesional sanitario afectado por el proceso. Como se verá en el siguiente capítulo, el paciente o usuario tiene derecho de acceso a su historia clínica y demás documentación médica sobre su persona, salvo que se aplique alguno de los límites previstos en la normativa de protección de datos o en la sanitaria. Los problemas se producen cuando es un tercero el que solicita acceder a la documentación de otra persona y llevarla al proceso judicial contra la voluntad del titular de la información. En la búsqueda del equilibrio entre los diferentes intereses jurídicos en juego hay que tener en cuenta que en cada jurisdicción la solución planteada será diferente. No se protegen los mismos bienes jurídicos en los procesos penales, civiles, administrativos o sociales[2542]. En principio, parece que la excepción al consentimiento que se estudia está pensada sólo para los procesos penales[2543]. No obstante, no se puede negar de partida la aplicación de esta excepción en las demás vías.

I.5.4.F.c.a´. En el ámbito civil.

En lo que corresponde a los procesos civiles la LEC establece un criterio sobre cómo se ha de actuar en caso de que una persona alegue la obligación o el derecho de guardar secreto. Primero, en el apartado dedicado a las diligencias preliminares, dispone la Ley que todo juicio puede prepararse mediante la petición de la historia clínica al centro sanitario o al profesional sanitario correspondiente[2544]. Parece, por lo tanto, que se abre la puerta a que el secreto pueda ser vulnerado o levantado. Y segundo, en el capítulo que regula los medios de prueba, esta Ley deja a criterio del tribunal la determinación de la conveniencia o no de respetar el secreto[2545]. Atendiendo a las características de cada caso se determinará si es necesario o no guardar el secreto médico en detrimento de la tutela judicial efectiva. De lo dicho resulta que la aportación de la historia clínica a los procesos civiles será posible según las circunstancias de cada supuesto, que deberá valorar el Juez o Tribunal pertinente. En todo caso, no se puede olvidar que en los procedimientos civiles la actuación de los juzgadores a la hora de solicitar cierta documentación está sometida, en la mayoría de supuestos[2546], a la voluntad de los intervinientes en el procedimiento, que serán quienes soliciten la práctica de las pruebas[2547].

Los tribunales no han tenido una línea de actuación regular o uniforme a la hora de interpretar estos preceptos. En la práctica, si se analiza la jurisprudencia son innumerables los supuestos en que se emplean datos extraídos de las historias clínicas para resolver conflictos. No parece que los órganos judiciales se planteen la posibilidad de no traer al proceso dichos datos como medio de prueba, previa valoración de si dicha actuación puede vulnerar el derecho a la intimidad o a la

[2542] RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente...,* cit., 2005, p. 221.
[2543] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 126.
[2544] Artículo 256.1 LEC: "*Todo juicio podrá prepararse; 5.bis) por la petición de la historia clínica al centro sanitario o profesional que la custodie, en las condiciones y con el contenido que establece la Ley*".
[2545] Artículo 371.1 LEC: *"cuando, por su estado o profesión, el testigo tenga el deber de guardar secreto respecto de hechos por los que se le interrogue, lo manifestará razonadamente y el tribunal, considerando el fundamento de la negativa a declarar, resolverá, mediante providencia, lo que proceda en Derecho. Si el testigo quedare liberado de responder, se hará constar así en el acta".*
[2546] Artículo 282 LEC: "*Las pruebas se practicarán a instancia de parte. Sin embargo, el tribunal podrá acordar, de oficio, que se practiquen determinadas pruebas o que se aporten documentos, dictámenes u otros medios e instrumentos probatorios, cuando así lo establezca la ley*". ILLESCAS RUS, *La Prueba Pericial…,* cit., 2002, p. 25; SEOANE SPIEGELBERG, *La Prueba en la Ley…,* cit., 2002, p. 21.
[2547] SAP de Guipúzcoa 29 de noviembre de 2004, FJ 3.

autodeterminación informativa de las personas[2548]. Y si bien en algún caso se ha hecho un llamamiento desde los propios órganos judiciales a la necesidad de respetar el principio de finalidad a la hora de emplear la historia clínica como medio de prueba[2549], lo cierto es que no existe una dinámica en la que se plantee, antes de traer este documento a juicio, un debate sobre si deben prevalecer los derechos a la autodeterminación informativa y a la intimidad. Sin embargo, frente a esa situación que parece generalizada, en algún caso se ha llevado a cabo una interpretación especialmente restrictiva del artículo 256.1.5.bis) de la LEC que regula las diligencias preliminares, generando cierta confusión. Concretamente, los tribunales han dado a entender en algún momento que ese precepto reconoce únicamente la posibilidad de que el paciente recabe su historia con el fin de preparar el proceso judicial y no a que sea un tercero quien lo haga, negando la facultad de este último a acceder a la documentación clínica de otro sujeto con el indicado fin[2550]. Lógicamente esta última interpretación no puede aceptarse como criterio generalizado a seguir por el juez civil, por cuanto anularía el derecho a la tutela judicial efectiva de quienes no siendo el titular de la historia necesitan acceder a la misma para defender su posición y preparar el proceso judicial. Bien sea en las diligencias preliminares o en la fase de prueba, el criterio a seguir ha de ser el de la necesidad de la documentación. Si una parte exige auxilio al órgano judicial correspondiente para obtener la historia clínica de un sujeto y presentarla al proceso, el órgano judicial no podrá negarse de partida a dicha actuación sino que deberá valorar si la diligencia es necesaria o no[2551].

La regulación llevada a cabo por la LEC es criticable. En primer lugar, puede ser cuestionable el que se deje en manos del juez o del magistrado esta decisión. Debería ser, en principio, el legislador el que determinase en una Ley cuándo debe ceder el secreto a favor de otros bienes jurídicos[2552]. La resolución de la colisión entre diferentes intereses ha de llevarse a cabo, cuando menos en la determinación de los principios que la han de guiar, en una Ley. Es esta norma la que tiene que establecer los límites de los derechos fundamentales. En segundo lugar, puede criticarse la ambigüedad del criterio que se define en el ordenamiento civil para resolver el conflicto que se formula. A la hora de decidir cómo se resuelve la colisión entre los diferentes bienes jurídicos, señala la normativa apuntada que queda en manos del Tribunal la decisión de levantar o no el secreto, atendiendo al fundamento que presente quien alega el secreto. Es fácilmente observable que no se definen unos criterios certeros sobre cuándo se preservará el deber de secreto.

[2548] SAP de Madrid 12 de diciembre de 2005, FJ 2. DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 553.
[2549] STS 25 febrero 2002, FJ 3: "la protección a la intimidad del paciente a través del secreto profesional y el carácter estrictamente reservado de los datos de la historia clínica salvo que los datos a los que se pretende acceder sean proporcionados y el acceso mismo necesario para atender finalidades dignas de protección en una sociedad democrática, deduciendo con toda claridad que no pueden exigirse inmotivadamente datos que no sean pertinentes para la finalidad de la investigación o cuya petición resulte especialmente inmotivada."
[2550] AAP de Álava 12 de marzo de 2010, FJ 2. El AAP de Barcelona 18 de abril de 2006, Parte Dispositiva, parece seguir un criterio diferente al acordar la aportación de la historia clínica de una persona solicitada por un tercero con el fin de impugnar un testamento.
[2551] BELLIDO PENADES, "Artículo 256…", cit., 2002, pp. 833 y siguientes.
[2552] DE LA OLIVA SANTOS, "Sección 7ª...", cit., 2001, p. 628, ha señalado acertadamente que no es precisamente la LEC la norma más adecuada para resolver estas cuestiones que "van más allá de una ley de enjuiciamiento".

Se entiende aquí que los órganos judiciales deben adoptar la decisión teniendo en consideración las circunstancias particulares que presente cada caso. Fundamentalmente, se debe tener en cuenta la importancia de los bienes jurídicos en juego. En el caso que se trata el secreto del médico salvaguarda lo que en la LOPD se califica como "datos especialmente protegidos". Parece clara la relevancia que se otorga en la norma a este tipo de información. No hay que dejar de subrayar que en muchas ocasiones los datos sanitarios afectarán a la intimidad de las personas. Piénsese en los casos en que se trata de datos referentes a la condición de un sujeto de portador del virus del VIH. Frente al interés de proteger la intimidad o derecho a la autodeterminación informativa se sitúa el derecho a la tutela judicial efectiva. Hay que tener en cuenta la cualidad de los intereses que se protegen en los procesos civiles. En la vía civil la tutela se dirige básicamente a la defensa de intereses particulares. Por definición, la vía civil está destinada a resolver los conflictos entre intereses privados[2553].

Lo dicho hasta ahora podría llevar a concluir que en los procesos civiles debe protegerse con mayor intensidad el deber de secreto profesional. Parte de la doctrina ha señalado que si la vulneración del deber de secreto va a tener como efecto inmediato la protección de intereses particulares, el punto de partida tiene que ser la reticencia a que se rompa el secreto[2554]. Según esta línea interpretativa prevalece el deber de secreto sobre la obligación de colaborar con la justicia. Este criterio ha de ser matizado. Hay que tener en cuenta que en la vía civil, si bien es cierto que de inicio no entra en juego el interés general, en sentido estricto, en ocasiones se protegen bienes jurídicos de especial relevancia. Piénsese, por ejemplo, en el caso en que se trata de determinar la paternidad de una persona[2555], o en el supuesto en que se pretende aclarar si un centro o profesional sanitario ha vulnerado el derecho a la intimidad de un paciente al haber revelado información sobre su vida privada[2556]. No cabe duda de que en estos casos se estará protegiendo un interés de particular importancia.

De lo expuesto hasta ahora se extrae la siguiente conclusión. Puede entenderse que en los procesos civiles el punto de partida sea el de la necesidad de salvaguardar el derecho a la protección de datos sanitarios de un paciente. Sin embargo, resulta indudable que el ordenamiento reconoce la posibilidad de que este principio se rompa, de tal forma que sea, en determinados casos, el derecho a la tutela judicial efectiva el que prevalezca sobre el deber de secreto. Se deja a criterio de Jueces y Tribunales la posibilidad de traer información sanitaria al proceso judicial. Y si bien en la práctica puede parecer que la manipulación de los datos sanitarios en los procesos judiciales es lo común, es necesario un ejercicio de ponderación para

[2553] Artículo 22 LOPJ.
[2554] LEGALIA, *La Protección...*, cit., 2002, p. 142, afirma que en los procesos civiles "-en que a diferencia del proceso penal, no se halla en juego el interés público en sentido estricto- puede el médico (y desde luego el hospital) invocar el secreto profesional para no suministrar la información confidencial que le haya sido solicitada".
[2555] STS 22 de marzo de 2001, FFJJ 3 y 4, en la que la negativa de un sujeto a someterse a una prueba de paternidad, junto a otras pruebas, como la información extraída de su historia clínica, llevan a admitir dicha paternidad.
[2556] SSTS 20 de abril de 2005, en la que se juzga un supuesto en que determinado centro reveló información sanitaria sobre un paciente; 27 de enero de 1997, en la que se analiza la responsabilidad de un centro por extraviar la historia clínica de un paciente que padecía Sida.

determinar si es posible la ruptura del deber de secreto de los profesionales sanitarios en beneficio del derecho a la tutela judicial efectiva[2557].

I.5.4.F.c.b´. El ámbito penal.

En el ámbito penal, los criterios que han de guiar la resolución de este conflicto varían con respecto a los que se acaban de plantear para la vía civil. De inicio, como ha señalado parte de la doctrina, parece que ha de otorgarse mayor relevancia al derecho a la tutela judicial efectiva[2558]. A la hora de resolver la colisión entre los diferentes bienes jurídicos en juego habrá que valorar dos situaciones conflictivas diferentes, pero que responden a argumentos semejantes.

A) En primer lugar, se encuentra el conflicto entre la obligación del profesional sanitario de denunciar los hechos delictivos de los que tenga conocimiento en el ejercicio de su profesión y el deber de guardar secreto.

Tanto la Constitución[2559] como el Código Penal[2560], así como la LECrim[2561] obligan, de inicio, a colaborar con la justicia en todo momento y a impedir que se puedan cometer delitos, teniendo que informar en todo caso sobre las posibles infracciones penales de las que se hubiera tenido conocimiento debido a la profesión de cada uno. En la normativa sanitaria se ha recogido en algún caso la obligación expresa de los profesionales sanitarios de denunciar y comunicar los hechos delictivos de los que tengan conocimiento[2562].

[2557] CRIADO DEL RIO, *Aspectos médico-legales…,* cit., 1999, p. 201.

[2558] Resolución AEPD, R/00645/2004, 26 de noviembre de 2004, procedimiento AAPP/00018/2004, FJ. 4; CANTERO RIVAS, "La Historia…", cit., 2004, p. 342: "en materia penal prevalece, a nuestro juicio, la averiguación de los delitos y el derecho a la tutela judicial efectiva sobre el secreto profesional".

[2559] Artículo 118 CE.

[2560] Artículo 450 CP: "*1. El que, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, será castigado con la pena de prisión de seis meses a dos años si el delito fuera contra la vida, y la de multa de seis a veinticuatro meses en los demás casos, salvo que al delito no impedido le correspondiera igual o menor pena, en cuyo caso se impondrá la pena inferior en grado a la de aquél.*
2. En las mismas penas incurrirá quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan un delito de los previstos en el apartado anterior y de cuya próxima o actual comisión tenga noticia".

[2561] Artículo 259 LECrim: obliga al que "*presenciare la perpetración de cualquier delito público (...) a ponerlo inmediatamente en conocimiento del Juez de instrucción, de Paz, Comarcal o Municipal, o Funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas*".
Artículo 262 LECrim: "*los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio, si se tratare de un delito flagrante.*
Los que no cumpliesen esta obligación incurrirán en la multa señalada en el artículo 259, que se impondrá disciplinariamente.
Si la omisión en dar parte fuere de un profesor de Medicina, Cirugía o Farmacia y tuviese relación con el ejercicio de sus actividades profesionales, la multa no podrá ser inferior a 125 pesetas ni superior a 250.
Si el que hubiese incurrido en la omisión fuere empleado público, se pondrá además, en conocimiento de su superior inmediato para los efectos a que hubiere lugar en el orden administrativo.
Lo dispuesto en este artículo se entiende cuando la omisión no produjere responsabilidad con arreglo a las leyes".

[2562] Artículo 12.2 de la reciente Ley 3/2005, de 8 de julio, de Extremadura de Información Sanitaria y Autonomía del Paciente: reconoce la *"obligación de los centros, establecimientos y servicios sanitarios de comunicación y denuncia en los supuestos previstos por la normativa aplicable, y especialmente en los casos de abusos, maltratos y vejaciones".*

Partiendo de estas premisas, parece clara la voluntad del legislador de que el deber de secreto ceda frente a la obligación de denunciar los hechos delictivos de los que se tiene conocimiento en el ejercicio de la profesión sanitaria. Esta posición podría estar justificada debido a que los intereses que se protegen en los procesos penales son de especial relevancia. Se está hablando de casos en que puede estar en juego, incluso, la vida de las personas.

A pesar de lo dicho, el propio ordenamiento abre la puerta a la posibilidad de que en determinados casos el deber de secreto prevalezca sobre la obligación de denunciar. La LECrim establece que los abogados, procuradores y eclesiásticos y ministros de culto quedan exentos de la obligación de colaborar e informar y denunciar[2563]. Esta previsión ha sido reforzada por la jurisprudencia que, en el caso de los abogados, ha subrayado el carácter inquebrantable de su deber de secreto[2564]. En algún momento se ha pretendido realizar una interpretación amplia del precepto incluyendo en este grupo a los profesionales sanitarios. Parte de la doctrina ha criticado que las normas que se han citado puedan acabar convirtiendo a estos últimos en delatores[2565]. Para evitar esta situación, se ha tratado de aplicar la excepción al deber de denunciar también a los profesionales de la sanidad. El argumento principal sería que en su caso, al igual que en los otros, la información la recibe el profesional debido a la relación de confianza que se da con el paciente[2566]. De esta forma, podría interpretarse que los profesionales sanitarios tampoco tienen obligación de denunciar los delitos de los que tengan conocimiento en el ejercicio de su cargo.

Se entiende aquí que esta interpretación no es posible. Se da una diferencia sustancial entre la situación de los profesionales sanitarios y los otros supuestos. En el caso de los primeros, el conocimiento de los hechos delictivos se produce mientras llevan a cabo su labor, pero esa información no se relaciona directamente con la actividad sanitaria. El conocimiento de ese hecho es puramente circunstancial. Piénsese en el caso en que un profesional sanitario descubre que una mujer ha sido objeto de malos tratos. La información no la extrae porque la mujer se lo ha contado, sino que la obtiene de forma circunstancial en la medida en que la asiste. En el caso de abogados y ministros de culto no ocurre así. En estos supuestos la información se obtiene porque el titular de los datos la transmite voluntariamente motivada por la función de aquéllos. Esta información será necesaria para que dichos profesionales puedan desarrollar su trabajo[2567]. Es el caso en que una persona admite haber cometido un delito ante estos profesionales, bien

[2563] Artículo 263 de la LECrim.: *"la obligación impuesta en el párrafo 1 del artículo anterior no comprenderá a los Abogados ni a los Procuradores respecto de las instrucciones o explicaciones que recibieron de sus clientes. Tampoco comprenderá a los eclesiásticos y ministros de cultos disidentes respecto de las noticias que se les hubieren revelado en el ejercicio de las funciones de su ministerio".*

[2564] SSTS 16 de diciembre de 2003, FJ 1; 3 de julio de 2008, FJ 2, en las que se subraya la obligación de los abogados de guardar secreto sobre los hechos y noticias que conozcan a raíz de su actuación profesional.

[2565] LEGALIA, *La protección...*, cit., 2002, p. 137, se refiere a este sanción, afirmando que "se trata de una regla –la mencionada- que no sólo no respeta el secreto profesional médico, sino que le obliga realmente a delatar"; SÁNCHEZ CARO y SÁNCHEZ CARO, *El Médico…,* cit., 2001, p. 111: "Se observará que tal precepto (la LECrim), que convierte a los médicos en delatores, choca abiertamente con la letra y el espíritu del precepto constitucional".

[2566] RIGO VALLBONA, *El secreto…,* cit., 1988, pp. 57-58; DE ANGEL YAGÜEZ, "Problemática de la Historia...", cit., 1997, p. 135, entiende que "la genérica expresión "secreto profesional" (...) tiene que acoger la actividad del médico, tan receptor de confidencias como el abogado o el sacerdote, confidencias que se le hacen en razón a una multisecular visión del profesional de la Medicina como alguien digno de recibir lo más íntimo de nuestra personalidad"; OTERO GONZÁLEZ, *Justicia y Secreto…,* cit., 2001, p. 33.

[2567] CORTÉS BECHIARELLI, *El Secreto Profesional…,* cit., 1998, p. 72, señala que estos "profesionales tantas veces señalados tienen conocimiento de esa materia –reservada o no-, exclusivamente, por y para ejercer su profesión".

para preparar la defensa o para confesarse por motivos religiosos. La comunicación de esta información viene motivada precisamente por la actividad que desempeñan dichos profesionales El conocimiento de informaciones delicadas es aquí parte de esa labor. En el caso de los profesionales sanitarios no es así. Quizás pudiera aceptarse que en el ámbito psiquiátrico se pueda alegar el deber de secreto para exceptuar la obligación de declarar. En este supuesto puede suceder que el conocimiento por el profesional de datos relacionados con la comisión de infracciones penales se deba al ejercicio de sus funciones. Sin embargo, más allá de este concreto caso, parece justificada la exclusión de estos últimos del ámbito de aplicación de la citada disposición de la LECrim.

Siendo difícil encajar a los profesionales sanitarios en el ámbito de aplicación de la excepción a la obligación a denunciar, hay argumentos suficientes para concluir que de inicio el deber de denunciar se impone al deber de secreto médico. No obstante, también aquí pueden establecerse matices. El hecho de que los profesionales sanitarios no se sitúen en las normas en el mismo grupo que los abogados o los eclesiásticos no quiere decir, que en ningún caso puedan argumentar el deber de secreto para evitar transmitir información sanitaria a los órganos judiciales y denunciar posibles delitos de los que tengan conocimiento. Las características particulares que puede presentar cada supuesto pueden decantar la solución en un sentido o en otro.

Como bien ha señalado algún autor, no es lo mismo, por ejemplo, dar a conocer hechos del pasado ya consumados, que hechos que pueden ocurrir en el futuro[2568]. En el primer caso sólo se estaría facilitando la investigación de un delito ya cometido. En el segundo, por el contrario, se podría estar evitando la comisión de un delito, que puede afectar incluso a la vida de las personas[2569]. Evidentemente, en este segundo supuesto la ruptura del secreto profesional está justificada. La naturaleza del delito que se pretende denunciar también ha de servir de parámetro a la hora de valorar si es necesaria o no la ruptura del deber de secreto. Los delitos afectan a distintos bienes jurídicos. No es lo mismo un hurto menor que un delito de lesiones graves. Puede entenderse que la ruptura del deber de secreto encuentra mayor fundamento en el segundo caso, en el que está en juego la integridad física de un sujeto, que en el primero, en el que se ve afectado, y no de una manera especialmente grave, el derecho a la propiedad privada. En última instancia, habrá que atender a la naturaleza de los datos que se han de transmitir a los órganos judiciales. Hay que tener en cuenta que, en estos supuestos, la obligación de informar se referirá, en la mayoría de casos, a los datos relacionados con la comisión de delitos, no tanto con la información sanitaria que recoge en el ejercicio de su profesión. No hay que olvidar que, atendiendo a los principios de calidad, los datos que se transmitirán serán los estrictamente necesarios para llevar a cabo el fin que se pretende[2570]. En la medida en que no se transmita información sanitaria, o la relevancia de estos datos sea menor, la obligación de denunciar tendrá mayor margen de actuación frente al deber de guardar secreto.

[2568] OTERO GONZÁLEZ, *Justicia y Secreto…,* cit., 2001, p. 35.
[2569] CRIADO DEL RIO, *Aspectos médico-legales…,* cit., 1999, p. 197; MUÑOZ CONDE, *Derecho Penal…,* cit., 2004, p. 268.
[2570] STS 25 de abril del 2000, FJ 1; SAP de Las Palmas 12 de septiembre de 2005, FJ 4.

Se entiende aquí, que si bien el ordenamiento parece reflejar una obligación genérica para los profesionales de la sanidad de denunciar los delitos de los que tengan conocimiento, este deber no puede entenderse de manera absoluta. También en la vía penal los órganos judiciales tendrán que realizar un ejercicio de ponderación dirigido a determinar, en cada caso, el alcance del deber de denunciar y del deber de secreto atendiendo a los criterios antedichos.

B) En segundo lugar, se encuentra el conflicto que en un determinado proceso puede generarse entre el deber de guardar secreto y la obligación del profesional sanitario de declarar como testigo o de aportar documentación con información sanitaria en un proceso judicial.

Cabe apuntar que cuando se hace referencia a la actuación del profesional como testigo no se está hablando de que el profesional actúe como perito[2571]. Cuando es llamado por los órganos judiciales o por una de las partes para ejercer como perito, el profesional desarrolla su actividad no con fines terapéuticos sino simplemente evaluativos. Es indudable que la relación entre el profesional sanitario y el sujeto evaluado es diferente a la que se da entre el profesional y un paciente que solicita un tratamiento médico. La obligación de guardar secreto sobre la información que resulta de la evaluación se relaja en la medida en que el profesional es llamado por los órganos judiciales o una de las partes en el devenir de un proceso judicial con el fin de llevar a cabo, simplemente, esta evaluación[2572]. En este sentido, en estos casos el profesional sanitario que le atienda estará obligado a remitir los resultados oportunos al órgano judicial que lo solicite[2573].

La LECrim establece como punto de partida la obligación de testificar y colaborar con la justicia en la resolución de cualquier conflicto[2574]. Sin embargo, frente a esa obligación genérica, en la misma Ley se encuentran disposiciones dirigidas a garantizar la institución del secreto profesional[2575]. No tienen obligación de declarar, entre otros, los funcionarios públicos. Si bien es

[2571] MORENA PÉREZ, "Secreto Médico…", cit., 2000, pp. 140-142.

[2572] Artículo 462 LECrim: "*Nadie podrá negarse a acudir al llamamiento del Juez para desempeñar un servicio pericial, si no estuviere legítimamente impedido*".

[2573] Artículo 355 LECrim: "*Si el hecho criminal que motivare la formación de una causa cualquiera consistiere en lesiones, los médicos que asistieren al herido estarán obligados a dar parte de su estado y adelantos en los períodos que se les señales, e inmediatamente que ocurra cualquier novedad que merezca ser puesta en conocimiento del Juez instructor*". AAP de Murcia 4 de octubre de 2010, FJ 1.

[2574] Artículo 410 LECrim: *"Todos los que residan en territorio español, nacionales o extranjeros, que no estén impedidos, tendrán obligación de concurrir al llamamiento judicial para declarar cuanto supieren sobre lo que les fuere preguntado si para ello se les cita con las formalidades prescritas en la Ley"*. Artículo 421 LECrim*, "el Juez de instrucción o municipal, en su caso, hará concurrir a su presencia y examinará a los testigos citados en la denuncia o en la querella o en cualesquiera otras declaraciones o diligencias y a todos los demás que supieren hechos o circunstancias, o poseyeren datos convenientes para la comprobación o averiguación del delito y del delincuente.*
Se procurará, no obstante, omitir la evacuación de citas impertinentes o inútiles".
Artículo 716 LECrim: *"el testigo que se niegue a declarar incurrirá en la multa de 200 a 5.000 euros, que se impondrá en el acto.*
Si a pesar de esto persiste en su negativa, se procederá contra él como autor del delito de desobediencia grave a la Autoridad".

[2575] Artículo 417 LECrim: *"No podrán ser obligados a declarar como testigos:*
1. Los eclesiásticos y ministros de los cultos disidentes, sobre los hechos que les fueren revelados en el ejercicio de las funciones de su ministerio.
2. Los funcionarios públicos, tanto civiles como militares, de cualquier clase que sean, cuando no pudieren declarar sin violar el secreto que por razón de sus cargos estuviesen obligados a guardar, o cuando, procediendo en virtud de obediencia debida, no fueren autorizados por su superior jerárquico para prestar la declaración que se les pida.

cierto que no todos los profesionales sanitarios son funcionarios, este precepto abre la puerta a que en algunos casos haya de respetarse el deber de secreto. Incluso, se ha pretendido realizar, con buen criterio, una interpretación amplia de esta norma incluyendo en ella a todos los profesionales de la sanidad, tengan o no vinculación con la Administración[2576].

La defensa o prevalencia del secreto sobre la obligación de testificar o aportar datos sanitarios de un paciente al proceso judicial podría tener su fundamento también en el Código Penal. Esta norma garantiza en determinadas disposiciones la vigencia del deber de secreto profesional sancionando la ruptura de dicho deber[2577]. Partiendo de esta regulación podría llegarse a entenderse que el transmitir datos sanitarios sobre una persona, incluso en un proceso judicial, constituye una actividad sancionable. Se entiende que el legislador no está pensando en el empleo de estos tipos penales a los casos que aquí se plantean. Es decir, resulta difícil que se puedan aplicar estas disposiciones a los supuestos en que un profesional sanitario transmite datos sanitarios en un proceso judicial con el fin de colaborar con la justicia. Si bien es cierto que no es necesario, para entender que existe delito, un elemento subjetivo especial de causar un daño[2578], la jurisprudencia ha interpretado que para que se considere cumplido el tipo penal es necesario que haya una intención clara de revelar los datos del paciente[2579]. Y en el supuesto que se trata no parece que la intención del profesional sanitario sea esa. No se cumple con el elemento subjetivo citado al trasladar información sanitaria de una persona a los órganos judiciales, cuando son llamados por estos últimos con la finalidad de colaborar con la justicia. El único supuesto en el que cabría aplicar estas disposiciones es el de la cesión de estos datos en dicho proceso desatendiendo claramente el principio de finalidad. Es decir, cuando transmite datos que nada tienen que ver con el correcto desarrollo del proceso.

En definitiva, el ordenamiento no aclara si en los procesos penales los profesionales sanitarios están obligados a actuar como testigos o a transmitir información sanitaria por

---

3. Los incapacitados física o moralmente".

[2576] GÓMEZ RIVERO, *La Protección…,* cit., 2007, p. 305.

[2577] Artículo 199 CP: *"1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.*
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años".

[2578] GÓMEZ RIVERO, *La Protección…*, cit., 2007, pp. 262-264. STS 4 de abril de 2001, FJ 2; SAP de Barcelona, 15 de septiembre de 2006, FJ 2: "la alegación recurrente vertida en soporte del motivo parte de una premisa errónea, cual es la afirmación de que el tipo penal del artículo 199.2 del Código Penal precisa para su realización de un elemento subjetivo proyectado sobre el injusto, elemento que se describe en el recurso como que la acción típica se lleve a cabo "con la finalidad de descubrir secretos o vulnerar la intimidad", así como con "conocimiento del perjuicio que podría causarse a la persona a la que afectaban los datos revelados"; pues bien, la sola lectura del precepto penal aplicado como infringido permite aseverar, a diferencia de lo que ocurre con el tipo penal sancionado en el artículo 197.1 y 2 del mismo Código –en que el legislador emplea los términos "para descubrir" o "en perjuicio de"-, que, en el plano subjetivo el delito de descubrimiento y revelación de secreto del artículo 199, no precisa para su acogimiento ningún elemento subjetivo que vaya más allá del dolo genérico exigido en los delitos dolosos, elemento éste que se satisfará, según ya se anticipa en la fundamentación de la resolución combatida, con el conocimiento y la voluntad del autor de proyectada sobre la situación típica, en este caso sobre la naturaleza íntima y reservada de los datos manejados por el autor, y sobre la situación profesional bajo la que se accede a esos datos".

[2579] SAP de Valencia 14 de mayo de 1999, FJ 4; Auto AP de de Madrid, 18 de junio de 2003, Fundamento de Derecho 1: es necesario para que exista el tipo penal "el elemento subjetivo, o intención clara y determinante de revelar un secreto que se conozca por razón del ejercicio de una determinada profesión que imponga el deber de sigilo".

requerimiento de los órganos judiciales, rompiendo su deber de secreto. La solución no aparece tan nítida en estos supuestos como en el caso anterior, en que la legislación parecía fijar con cierta claridad la obligación de los profesionales sanitarios de denunciar los hechos delictivos de los que tuvieran conocimiento. La ambigüedad de la normativa es notable y no se adivina cuál ha de ser el criterio que deban seguir los órganos judiciales para determinar qué interés ha de prevalecer. En la práctica parece dejarse al arbitrio de Jueces y Tribunales la resolución de este conflicto. Y, como sucedía en el orden civil, el uso viene siendo el de aportar la información necesaria a los procesos, sin que se plantee la posibilidad de que prevalezca el deber de secreto de los profesionales. En esta línea, los tribunales han admitido la acción de entrada y registro en los centros sanitarios como medio para investigar los delitos, sin considerar que dicha actividad pueda vulnerar el deber de secreto[2580].

Ante el marco dispuesto por el ordenamiento, la solución al conflicto jurídico planteado en este apartado pasa, como ocurriera en los demás casos, por ponderar los diferentes intereses que entran en juego en cada caso concreto[2581]. En primer lugar, hay que tener en cuenta que en los procesos penales se están protegiendo bienes jurídicos de especial relevancia. Además, más allá de los intereses particulares que pueden estar en juego en cada proceso concreto, en la vía penal se están marcando los límites del comportamiento de los sujetos que componen la sociedad para que sea posible la convivencia. Se protege por lo tanto, aunque sea de forma mediata, un interés general. Este hecho hace que el punto de partida a la hora de dirimir el conflicto que se plantea pueda ser la obligación de aportar al proceso todos los datos de los que se pueda disponer para el correcto desarrollo de la investigación penal[2582]. No obstante, más allá de este punto de partida habrá que estar a las características propias de cada proceso. En este sentido, hay que tomar en consideración, en segundo lugar, la sensibilidad de la información sanitaria que se solicita y la entidad del bien jurídico que se pretende proteger con la investigación. No será lo mismo trasladar a un proceso el dato de que una persona ha pasado un proceso gripal, que transmitir la información de que es seropositivo. Y tampoco tendrá las mismas consecuencias que se esté investigando un supuesto de hurto menor que un caso de violación.

I.5.4.F.c.c´. En la vía administrativa.

En la vía administrativa el acceso a la información sanitaria puede ser también relevante. Tanto en determinados procedimientos sancionadores, como en procedimientos dirigidos a aclarar una posible responsabilidad patrimonial de la Administración sanitaria, el acceso a información sobre la salud de determinadas personas puede resultar fundamental. En el primer caso, cuando se trata de sancionar a una persona por haber cometido una infracción de la normativa sanitaria, es lógico pensar que conocer determinados datos de salud puede ser de

[2580] STC 15 de febrero de 1989, FJ 4.
[2581] MUÑOZ CONDE, *Derecho Penal…,* cit., 2004, p. 268; EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 38. Ocurre lo mismo en otros supuestos en que se llevan a cabo actuaciones que invaden la intimidad de las personas con el fin de obtener pruebas o indicios sobre determinados hechos. Es el caso de la invasión del domicilio o las telecomunicaciones, SSTS 19 de febrero de 2003, FJ 1; 14 de noviembre de 2007, FJ 2.
[2582] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 126; DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 548.

utilidad. Piénsese en el supuesto de un médico que ha cometido una infracción y para conocer las circunstancias que rodean al caso es necesario acceder a la historia clínica de un paciente determinado. En el segundo ocurre lo mismo. La LPAC dispone que responde la Administración por la actuación de las personas que "están a su servicio"[2583]. La interpretación que se ha de dar a ese concepto, según la doctrina, tiene que ser amplia[2584]. La actuación de los profesionales sanitarios al servicio de la Administración pública, por lo tanto, puede generar, si se dan los requisitos necesarios, responsabilidad patrimonial de la Administración. De hecho, en la práctica, son numerosos los litigios que se producen en la actualidad en relación al mal funcionamiento de la Administración sanitaria[2585]. Según la Ley, esta responsabilidad se producirá tanto por la actuación normal como anormal de estos sujetos[2586], siempre y cuando se produzcan lesiones[2587]. Para determinar la existencia o no de estas lesiones y la cuantía de la indemnización pertinente serán necesarios todos los medios de prueba. Precisamente, entre estos medios se encuentra la información sanitaria contenida, básicamente, en las historias clínicas[2588].

En lo que concierne a la actividad de la Administración habría que distinguir dos ámbitos de actuación. El traslado de información sanitaria a un proceso con el fin de controlar la actuación del aparato público puede darse en un procedimiento administrativo o en un proceso judicial contencioso-administrativo. En relación al primero, la norma que regula el desarrollo del procedimiento de responsabilidad patrimonial de la Administración simplemente hace referencia a la necesidad de practicar las pruebas que se hayan declarado necesarias[2589]. Sin embargo, en el ámbito autonómico alguna norma ha reconocido expresamente la facultad de la Administración de acceder a la historia clínica de un paciente para resolver un supuesto de responsabilidad patrimonial[2590]. En lo que corresponde al procedimiento sancionador ocurre lo mismo. La

[2583] Artículo 144, LPAC: "*Cuando las Administraciones públicas actúen en relaciones de derecho privado, responderán directamente de los daños y perjuicios causados por el personal que se encuentre a su servicio (…)*".

[2584] MARTÍN REBOLLO, "La responsabilidad…", cit., 1994, p. 48; SÁNCHEZ MORÓN, *Derecho Administrativo…,* cit., 2007, pp. 905-906; GARCÍA CÓMEZ de MERCADO, *Responsabilidad Patrimonial…,* cit., 2009, p. 30.

[2585] MORENO MOLINA y MAGÁN PERALES, *La Responsabilidad Patrimonial…,* cit., 2005, p. 389; ARQUILLO COLET, *Seguro y Responsabilidad Patrimonial…,* cit., 2008, p. 205; GARCÍA CÓMEZ de MERCADO, *Responsabilidad Patrimonial…,* cit., 2009, p. 219.

[2586] Artículo 139.1 LPAC: "*Los particulares tendrán derecho a ser indemnizados por las Administración públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, salvo en los casos de fuerza mayor, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos*". GARCÍA CÓMEZ de MERCADO, *Responsabilidad Patrimonial…,* cit., 2009, p. 31.

[2587] Artículo 139.2 LPAC: "*En todo caso, el daño alegado habrá de ser efectivo, evaluable económicamente e individualizado con relación a una persona o grupo de personas*". DE AHUMADA RAMOS, *La Responsabilidad Patrimonial…,* cit., 2004, p. 147.

[2588] DE LORENZO Y MONTERO, *Derechos y Obligaciones…*, cit., 2003, p. 127.

[2589] Artículo 9 RD 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los Procedimientos de las Administraciones Públicas en materia de Responsabilidad: "*En el plazo de treinta días se practicarán cuantas pruebas hubieran sido declaradas pertinentes. (…)*". Artículo 10 RD 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los Procedimientos de las Administraciones Públicas en materia de Responsabilidad: "*El órgano competente para la instrucción del procedimiento podrá solicitar cuantos informes estime necesarios para resolver*".

[2590] Artículo 19 Ley 3/2001, de Galicia, de 28 de mayo de 2001, del Consentimiento Informado y de la Historia Clínica de los Pacientes: "*2. En los supuestos de procedimientos administrativos de exigencia de responsabilidad patrimonial o en las denuncias previas a la formalización de un litigio sobre la asistencia sanitaria se permitirá que el paciente tenga acceso directo a la historia clínica, en la forma y con los requisitos que se regulen legal o reglamentariamente. También tendrán acceso a la historia clínica los órganos competentes para tramitar y resolver los procedimientos de responsabilidad patrimonial por el funcionamiento de la Administración sanitaria, así como la inspección sanitaria en el ejercicio de sus funciones*". Artículo 14 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el uso y acceso a la historia clínica electrónica: "*En los supuestos de procedimientos administrativos de exigencia de*

normativa no hace referencia alguna al problema que ahora se plantea. Se señala simplemente que se practicarán las pruebas que se estimen pertinentes para determinar los hechos y las responsabilidades[2591]. En normas sectoriales se refrenda esta posibilidad abogando porque se recabe toda la información posible[2592]. En caso de rechazar la realización de una prueba el instructor deberá motivar su decisión[2593]. En la práctica, en algún caso las agencias de protección de datos se han pronunciado a este respecto a favor de que se traslade la información sanitaria pertinente a los órganos administrativos[2594].

Por su parte, la Ley que regula el procedimiento a seguir en la jurisdicción contencioso-administrativa simplemente habla de la posibilidad de aportar pruebas a dicho proceso, sin que se establezca límite alguno a esta fase[2595]. También señala la obligación de aportar al proceso contencioso-administrativo el expediente administrativo correspondiente[2596]. Algunos autores han concluido, partiendo de estas consideraciones, que resulta normal la aportación a estos procesos de la historia clínica[2597]. Como se ve, la normativa que regula el desarrollo de ambos procedimientos no entra a analizar la cuestión que aquí se trata. Tampoco la jurisprudencia ni la doctrina han profundizado sobre esta cuestión. Está situación, genera una inseguridad jurídica que ha sido puesta de manifiesto incluso por los tribunales[2598].

A falta de previsión legal, las interpretaciones que se puedan realizar al respecto no pueden ser definitivas. A) En relación a los casos en que se pretenden transmitir datos sanitarios a un órgano administrativo la cuestión es especialmente compleja. En primer lugar, no hay que olvidar

---

responsabilidad patrimonial sobre la asistencia sanitaria se permitirá que los órganos competentes para su tramitación y resolución tengan acceso a la información contenida en la historia clínica electrónica, limitado estrictamente a los fines específicos de cada caso".

[2591] Artículo 137.4 LPAC: "*Se practicarán de oficio o se admitirán a propuesta del presunto responsable cuantas pruebas sean adecuadas para la determinación de hechos y posibles responsabilidades. Sólo podrán declararse improcedentes aquellas pruebas que por su relación con los hechos no puedan alterar la resolución final a favor del presunto responsable*".

[2592] Artículo 124 RDLOPD: "*Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados*".

[2593] Artículo 80.3 LPAC: "*El instructor del procedimiento sólo podrá rechazar las pruebas propuestas por los interesados cuando sean manifiestamente improcedentes o innecesarias, mediante resolución motivada*"; artículo 137.4 LPAC.

Artículo 37.1.a) Ley 2/1998, 20 de febrero, de la Potestad Sancionadora de las Administraciones Públicas de la Comunidad Autónoma del País Vasco: "*El instructor motivará sus decisiones de inadmisión de la solicitud de apertura de período probatorio y de rechazo de pruebas concretas, en aplicación de los artículos 80 y 137.4 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común".*

[2594] Resolución APDCM, 18 de septiembre de 2009, "La potestad sancionadora de una Administración habilita la utilización de datos personales para el esclarecimiento de los hechos".

[2595] Artículos 60 y 61 LJCA.

[2596] Artículos 45 y siguientes LJCA.

[2597] CANTERO RIVAS, "El contenido de la historia…", cit., 2004, p. 416; DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 550.

[2598] STSJ de Castilla la Mancha, de 2 de junio de 2003, FJ. Único: "la conducta del recurrente, de negarse al requerimiento realizado (a que ceda información sanitaria de sus pacientes a la Administración Sanitaria), no puede ser sancionada pues no concurre el necesario elemento subjetivo de la culpabilidad. Por cuanto se produce tras una duda razonable sobre si al cumplir el mismo podía vulnerar el derecho a la intimidad de sus pacientes y el deber de secreto profesional".

que se está tratando de datos que son considerados por el ordenamiento como especialmente protegidos. En segundo lugar, hay que tener en cuenta que se trata de resolver un procedimiento administrativo, no un proceso judicial. Ni la LOPD ni la LBAP prevén el acceso de órganos administrativos a la historia clínica con estos fines.

A favor de la necesidad de romper el deber de secreto podrían buscarse diferentes argumentos. Podría alegarse que la aportación de la historia clínica al procedimiento administrativo constituye una cesión con finalidad inspectora justificada por la Ley estatal[2599]. Difícilmente, se entiende aquí, puede interpretarse el supuesto que se analiza como un procedimiento con finalidad inspectora. Ni el ejercicio de la potestad sancionadora, ni la función de aclarar supuestos de responsabilidad patrimonial responden a dicha finalidad[2600]. Podría plantearse también para estos supuestos la aplicabilidad de la excepción relativa a la cesión de datos entre administraciones. En contra de este argumento cabe recordar que en lo referente a los datos de salud se entendía que esta excepción sólo se aplica con fines sanitarios. No parece, en términos genéricos, sencillo plantear una base jurídica que apoye la transmisión de los datos sanitarios a órganos administrativos con los fines que ahora se comentan.

Más allá de lo expuesto, los argumentos a favor de trasladar datos sanitarios a órganos administrativos para resolver procedimientos de responsabilidad patrimonial pueden ser varios. Primero, cuando se tratan de aclarar supuestos de responsabilidad patrimonial se ha visto que pueden encontrarse referencias normativas que expresamente exigen la revelación de datos. Podría argumentarse que la excepción al consentimiento tiene fundamento, en este caso, en la previsión de la LOPD que reconoce la posibilidad de limitar el derecho a consentir una cesión de datos de salud cuando una Ley, por motivos de interés general, así lo prevea. No obstante, esta consideración ha de ser matizada. No se puede obviar que lo dispuesto por la norma gallega constituye un nuevo límite a los derechos de intimidad y autodeterminación informativa, que no encuentra reflejo ni en la LOPD, ni en la LBAP, ni en las demás normas autonómicas conocidas. Esta situación genera cierta inquietud a la hora de determinar su validez, fundamentalmente debido a que no se reconoce el bien jurídico que se protege con la aplicación del límite. Segundo, en algún caso la jurisprudencia se ha apoyado en la normativa administrativa arriba citada, que regula el procedimiento de solicitud de responsabilidad patrimonial de la Administración, para justificar la excepción al consentimiento[2601]. Lo cierto es que dar carta blanca a este tipo de transferencias basándose en preceptos tan ambiguos, que no hacen referencia alguna a las historias clínicas, genera ciertas dudas. Tercero, también se ha planteado en alguna ocasión la posibilidad de limitar el derecho al consentimiento en atención a que la cesión se dirige a controlar la relación jurídica creada entre el centro y el paciente, basándose en el artículo 11.2.c) LOPD. El procedimiento de responsabilidad patrimonial no sería más que una vía para determinar los parámetros entre los que se ha producido dicha relación[2602]. Ya se ha comentado la duda que surge al cuestionar la aplicabilidad de este precepto a las cesiones de los datos de

[2599] Artículo 16.5 LBAP. TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, p. 239.
[2600] ALARCÓN SOTOMAYOR, *El Procedimiento Administrativo…,* cit., 2007, p. 202.
[2601] SAN 18 de febrero de 2009, FJ 3.
[2602] Resolución APDCM, "Cesión de documentación clínica a diversos órganos de la Administración de la Comunidad de Madrid que están tramitando procedimientos de responsabilidad patrimonial", 2007.

salud, por lo que no parece que sea éste un argumento definitivo que favorezca la comunicación de datos sanitarios con este fin. Quizás podría argumentarse, en los casos en que se solicita a un profesional sanitario que remita unos datos de carácter personal con el fin de aclarar la posible responsabilidad de la Administración pertinente, que el fin último que se persigue con el procedimiento no es otro que mejorar la calidad del sistema sanitario.

Cuando se trata de ejercer la potestad sancionadora el planteamiento es también dudoso. En este caso no se observa norma alguna que permita este tipo de comunicaciones a órganos administrativos, aunque pueden encontrarse argumentos favorables a la cesión de datos. Primero, podría pensarse que el adecuado ejercicio de la potestad sancionadora repercute en última instancia en el buen funcionamiento de la Administración. Como se viera al analizar las cesiones a favor de los Colegios Profesionales, la actividad sancionadora tiene como fin mediato la determinación de cuál es el correcto comportamiento de quienes actúan dentro de un sistema sanitario. Segundo, hay que tener en cuenta que se está hablando de un procedimiento que puede llevar a sancionar a una persona. El carácter gravoso de este resultado hace que sea necesario que también en este procedimiento se adopten una serie de garantías. Así se ha estimado en algún informe de la AEPD, que ha admitido el traslado de determinados datos sanitarios a un procedimiento disciplinario, argumentando que lo contrario generaría una situación de inseguridad para el sujeto investigado[2603]. Es así que, como bien han señalado la jurisprudencia y la doctrina, son aplicables a estos procedimientos los principios que se recogen en los artículos 24 y 25 CE, entre ellos el de la tutela judicial efectiva[2604]. No obstante, no es menos cierto que estos principios no operan de igual manera en la vía penal y en los procedimientos administrativos, tal como han reconocido los mismos tribunales[2605]. Esto se debe, fundamentalmente, a que la complejidad de un proceso judicial no se reproduce en un procedimiento sancionador administrativo, de manera tal que sea difícil equiparar las garantías que se dan en uno y otro[2606]. No parece que un órgano administrativo, compuesto por funcionarios o cargos políticos, ofrezca las mismas garantías a la hora de decidir si hay que revelar determinados datos de salud para llevar a cabo un procedimiento administrativo. La prueba es que, como ya se ha señalado, en otras injerencias en el derecho a la intimidad son los Jueces y Magistrados quienes deberán autorizar la invasión. Además, tampoco hay que olvidar que ese mismo artículo 24, aplicable en este tipo de procedimientos, reconoce también el deber de secreto.

En ámbitos de actuación diferentes, como el comentado tributario, la obligación de colaborar con la Administración es absoluta[2607]. Sin embargo, esto no puede servir de argumento definitivo para admitir que los datos sanitarios han de ser transmitidos a la Administración en los casos que

[2603] Informe jurídico AEPD 0400/2008.
[2604] STC 15 de junio de 2009, FJ 4. LASAGABASTER HERRARTE, "Artículo 2…", cit., 2006, p. 95; ALARCÓN SOTOMAYOR, *El Procedimiento Administrativo…,* cit., 2007, p. 31.
[2605] STC 26 de abril de 1990, FJ 10, señala que hay que tener prudencia al trasladar estos principios al ámbito del procedimiento administrativo. Resolución APDCM, 23 de diciembre de 2009, "Si no hay tratamiento de datos no existe obligación de declarar el fichero".
[2606] STC 16 de enero de 2003, FJ 8. ALARCÓN SOTOMAYOR, *El Procedimiento Administrativo…,* cit., 2007, p. 39; CUBERO MARCOS, *El Principio…,* cit., 2010, pp. 110-111.
[2607] ALARCÓN SOTOMAYOR, *El Procedimiento Administrativo…,* cit., 2007, p. 237.

ahora se analizan. Es cierto que la Administración tiene acceso a la información económica de los ciudadanos, que, como se ha citado más arriba, se ven obligados a colaborar con aquélla. En este caso, sin embargo, la transmisión de datos se erige en pieza fundamental para que la Administración pueda llevar a cabo su labor[2608], labor que tiene su fundamento en la mismísima norma suprema que reconoce el deber de todos a colaborar en el sostenimiento de los gastos públicos[2609]. Por otro lado, se está hablando en este caso de transmitir datos económicos, que, la mayoría de veces, no tienen en la Ley la consideración de datos especialmente protegidos. Hay que recordar que las leyes disponen la obligación expresa de transmitir los datos necesarios a la Administración tributaria para que ésta pueda llevar a cabo sus funciones[2610], cosa que no ocurre en el supuesto que aquí se analiza. Por último, se ha de tener en consideración que los profesionales sanitarios están sujetos a un deber de secreto de especial vigor debido a las características de la información que manejan.

Teniendo en cuenta todo lo dicho parece que en los procedimientos administrativos la vigencia del deber de secreto médico ha de prevalecer sobre la obligación de transmitir la información sanitaria. No hay que olvidar que se está tratando en este momento de un simple procedimiento administrativo, no de un proceso judicial en el que se garantiza que los órganos judiciales llevarán a cabo el ejercicio de ponderación adecuado[2611]. No obstante también aquí pueden encontrarse argumentos favorables a la necesidad de que el ejercicio de ponderación

[2608] ORTIZ LIÑÁN, *Derechos y garantías…,* cit., 2003, p. 2.

[2609] Artículo 31 CE.

[2610] Artículo 29.2 Ley 58/2003, 17 de diciembre, General Tributaria: "*2. Además de las restantes que puedan legalmente establecerse, los obligados tributarios deberán cumplir las siguientes obligaciones:*
a)La obligación de presentar declaraciones censales por las personas o entidades que desarrollen o vayan a desarrollar en territorio español actividades u operaciones empresariales y profesionales o satisfagan rendimientos sujetos a retención.(…)
c)La obligación de presentar declaraciones, autoliquidaciones y comunicaciones.
d)La obligación de llevar y conservar libros de contabilidad y registros, así como los programas, ficheros y archivos informáticos que les sirvan de soporte y los sistemas de codificación utilizados que permitan la interpretación de los datos cuando la obligación se cumpla con utilización de sistemas informáticos. Se deberá facilitar la conversión de dichos datos a formato legible cuando la lectura o interpretación de los mismos no fuera posible por estar encriptados o codificados.
En todo caso, los obligados tributarios que deban presentar autoliquidaciones o declaraciones por medios telemáticos deberán conservar copia de los programas, ficheros y archivos generados que contengan los datos originarios de los que deriven los estados contables y las autoliquidaciones o declaraciones presentadas.
e)La obligación de expedir y entregar facturas o documentos sustitutivos y conservar las facturas, documentos y justificantes que tengan relación con sus obligaciones tributarias.
f)La obligación de aportar a la Administración tributaria libros, registros, documentos o información que el obligado tributario deba conservar en relación con el cumplimiento de las obligaciones tributarias propias o de terceros, así como cualquier dato, informe, antecedente y justificante con trascendencia tributaria, a requerimiento de la Administración o en declaraciones periódicas. Cuando la información exigida se conserve en soporte informático deberá suministrarse en dicho soporte cuando así fuese requerido.
g)La obligación de facilitar la práctica de inspecciones y comprobaciones administrativas.
h)La obligación de entregar un certificado de las retenciones o ingresos a cuenta practicados a los obligados tributarios perceptores de las rentas sujetas a retención o ingreso a cuenta.(…)". SAN 23 de octubre de 2006, FJ 4, en la que se subraya el hecho de que el ordenamiento impone la obligación de facilitar información a la Administración tributaria. GONZÁLEZ MÉNDEZ, *La Protección de Datos…,* cit., 2003, p. 69, señala que la excepción al consentimiento se justifica también por el hecho de que el tratamiento se lleva a cabo por la Administración en el ejercicio de sus funciones.

[2611] STC 23 de marzo de 2009, FJ 4, señala que la transmisión de datos de salud a la Administración ha de cumplir estrictas garantías. La cesión ha de estar prevista expresamente en la Ley y responder a motivos concretos de cierta entidad.

haya de hacerse caso por caso. Como se puede intuir, tanto en los procedimientos sancionadores, como en los dirigidos a determinar la posible responsabilidad patrimonial de la Administración, lo que en última instancia está en juego es la determinación de cuáles han de ser los parámetros entre los que puede actuar, en este caso, la Administración sanitaria. Es decir, se están marcando los criterios que han de guiar el buen funcionamiento de esta Administración. Esta finalidad bien puede merecer en determinados casos que se dé traslado de cierta información sanitaria a favor de órganos administrativos. Evidentemente, estos supuestos se limitarán a circunstancias en que el bien común pueda beneficiarse de manera clara de esa cesión y la intimidad o el derecho a la autodeterminación informativa del sujeto afectado no se vea perjudicado de manera especialmente grave. En todo caso, habrá que plantear que deberá ser un órgano externo a la Administración cuyo funcionamiento se cuestiona el que determine qué interés prevalece, sea un órgano judicial o una Administración independiente como una agencia de protección de datos.

B) Algo parecido ocurre cuando se trata del proceso contencioso administrativo, donde es un órgano judicial quien solicita o aprueba la necesidad de que se traiga cierta información sanitaria al proceso. Como se ha visto, el ordenamiento no aclara nada sobre el conflicto planteado. Tampoco la doctrina que ha analizado el proceso contencioso administrativo ha dedicado especial atención a esta cuestión[2612], si bien en algún caso, basándose en el artículo 48 LJCA[2613],

[2612] LESMES SERRANO, "Prueba…", cit., 1998; GARCÍA GIL, *El Proceso Contencioso…,* cit., 1998, p. 599; AYALA MUÑOZ, "Artículos 60 y 61. Prueba…", cit., 1999; AGÚNDEZ FERNÁNDEZ, *Ley 29 de 13 de julio de 1998…,* cit., 1998, p. 367; PERA VERDAGUER, *Comentarios a la Ley…,* cit., 2004; GONZÁLEZ RIVAS y ARANGUREN PÉREZ, *Comentarios a la Ley...*, cit., 2006;

[2613] Artículo 48 LJCA: *"1. El órgano jurisdiccional, al acordar lo previsto en el apartado 1 del artículo anterior, o mediante resolución si la publicación no fuere necesaria, requerirá a la Administración que le remita el expediente administrativo, ordenándole que practique los emplazamientos previstos en el artículo 49. El expediente se reclamará al órgano autor de la disposición o acto impugnado o a aquél al que se impute la inactividad o vía de hecho. Se hará siempre una copia autentificada de los expedientes tramitados en grados o fases anteriores, antes de devolverlos a su oficina de procedencia.*

2. No se reclamará el expediente en el caso del apartado 2 del artículo anterior, sin perjuicio de la facultad otorgada por el apartado 5 de este artículo 48.

3. El expediente deberá ser remitido en el plazo improrrogable de veinte días, a contar desde que la comunicación judicial tenga entrada en el registro general del órgano requerido. La entrada se pondrá en conocimiento del órgano jurisdiccional.

4. El expediente, original o copiado, se enviará completo, foliado y, en su caso, autentificado, acompañado de un índice, asimismo autentificado, de los documentos que contenga. La Administración conservará siempre el original o una copia autentificada de los expedientes que envíe. Si el expediente fuera reclamado por diversos Juzgados o Tribunales, la Administración enviará copias autentificadas del original o de la copia que conserve.

5. Cuando el recurso contra la disposición se hubiere iniciado por demanda, el Tribunal podrá recabar de oficio o a petición del actor el expediente de elaboración. Recibido el expediente, se pondrá de manifiesto a las partes por cinco días para que formulen alegaciones.

6. Se excluirán del expediente, mediante resolución motivada, los documentos clasificados como secreto oficial, haciéndolo constar así en el índice de documentos y en el lugar del expediente donde se encontrarán los documentos excluidos.

7. Transcurrido el plazo de remisión del expediente sin haberse recibido completo, se reiterará la reclamación, y si no se enviara en el término de diez días contados como dispone el apartado 3, tras constatarse su responsabilidad, previo apercibimiento notificado personalmente para formulación de alegaciones, se impondrá una multa coercitiva de 300,50 a 1.202,02 € a la autoridad o empleado responsable. La multa será reiterada cada veinte días, hasta el cumplimiento de lo requerido.

De darse la causa de imposibilidad de determinación individualizada de la autoridad o empleado responsable, la Administración será la responsable del pago de la multa sin perjuicio de que se repercuta contra el responsable.

se ha entendido que la aportación de la historia clínica es preceptiva[2614]. Se ha interpretado que la historia clínica, en los procedimientos de exigencia de responsabilidad patrimonial, es parte de los expedientes administrativos a los que se cita en dicho precepto y, siendo así, ha de ser entregada a los órganos judiciales en todo caso, pues así lo exige la Ley. No obstante, este hecho no puede suponer que en estos procesos el deber de secreto de los profesionales sanitarios no tenga vigencia alguna. Evidentemente, si en los procesos penales y civiles se plantean serias dudas sobre la conveniencia o no de romper este deber de secreto, lo mismo ocurre en este orden. De hecho, el artículo 60.4 de la LJCA realiza una remisión a la normativa civil a la hora de determinar el régimen jurídico a seguir en la regulación de la fase de prueba[2615].

En la mayoría de casos, tanto cuando se trata de un supuesto caso de responsabilidad patrimonial como cuando concierne a un proceso sancionador, lo que se trata de proteger de manera inmediata en estos procesos judiciales es el interés de un sujeto que ha sufrido un daño por una determinada actuación de la Administración, bien porque le ha impuesto una sanción, o porque esta última ha llevado a cabo una acción u omisión que ha generado una lesión a dicho sujeto. Sin embargo, más allá de este interés particular, en muchas ocasiones se ha hablado de que el bien jurídico en juego en este tipo de procesos es el buen funcionamiento de la Administración, en este caso, de la Administración sanitaria, o la fijación de los límites del comportamiento de los ciudadanos. De esta forma, aunque sea de manera mediata, lo que se está protegiendo no es otra cosa que un interés general o común.

Se podría establecer como punto de partida la obligación de ceder los datos sanitarios a los Jueces y Magistrados. No obstante, como ocurriera en las otras jurisdicciones, se plantea la necesidad de un análisis más profundo por parte de estos órganos en cada proceso. La posibilidad de vulnerar la intimidad de las personas en beneficio de un bien tan abstracto como el buen funcionamiento de la Administración tiene que llevar a la obligación de los órganos judiciales, de tener que cuestionarse en cada caso la conveniencia de romper el deber de secreto. En este sentido, deberán analizar por un lado la entidad de la información sanitaria que se solicita y, por otro, en qué medida puede beneficiar la cesión de los datos al buen desarrollo de cada proceso.

I.5.4.F.d. Requisitos generales que han de cumplir las cesiones a los órganos judiciales.

Se han aportado hasta ahora unos criterios que pueden ayudar, de alguna manera, a resolver el conflicto que en las distintas vías jurídicas se puede plantear entre distintos bienes jurídicos

8. Contra los autos en los que se acuerde la imposición de multas a las que se refiere el apartado anterior podrá interponerse recurso de súplica en los términos previstos en el artículo 79.
9. Si no se hubieran satisfecho voluntariamente, las multas firmes se harán efectivas por vía judicial de apremio.
10. Impuestas las tres primeras multas coercitivas sin lograr que se remita el expediente completo, el Juez o Tribunal pondrá los hechos en conocimiento del Ministerio Fiscal, sin perjuicio de seguir imponiendo nuevas multas. El requerimiento cuya desatención pueda dar lugar a la tercera multa coercitiva contendrá el oportuno apercibimiento".
[2614] CANTERO RIVAS, "La historia clínica…", cit., 2002, p. 230.
[2615] Artículo 60.4 LJCA: "*La prueba se desarrollará con arreglo a las normas generales establecidas para el proceso civil, si bien el plazo será de quince días para proponer y treinta para practicar. No obstante, se podrán aportar al proceso las pruebas practicadas fuera de este plazo por causas no imputables a la parte que las propuso*". GONZÁLEZ PÉREZ, *Comentarios a la Ley…,* cit., 1998, p. 1152.

que chocan entre sí, fundamentalmente el derecho a la tutela judicial efectiva y el deber de secreto. Más allá de estos criterios cabe realizar una serie de apuntes que deberán tomarse en consideración en todo proceso en que colisionen los citados intereses.

A) En primer lugar, la excepción al consentimiento en estos supuestos se aplicará cuando la cesión se produzca directamente a favor de los jueces y tribunales. Es decir, no es necesario el consentimiento cuando son los Jueces y Tribunales los que solicitan la información. Este requerimiento se deduce de las normas y se ha puesto de manifiesto en la jurisprudencia[2616]. Es importante subrayar esta idea porque la excepción no se aplica cuando el destinatario primero de los datos es otro sujeto diferente a los citados. No es posible, por ejemplo, aplicar esta excepción a los casos en que la cesión se da de un particular a otro, para que este segundo pueda emplear la información como elemento probatorio en un proceso judicial determinado. Para aplicar el límite al derecho a consentir una cesión la comunicación ha de darse a favor, directamente, de los órganos judiciales. Tiene sentido esta interpretación en la medida en que la excepción que se aplica viene motivada, fundamentalmente, por el hecho de que la labor de estos sujetos se relaciona con el ámbito de la justicia y la defensa de los derechos fundamentales de los ciudadanos.

B) En segundo lugar, hay que tener en cuenta que los principios básicos que determinan la calidad de los datos han de informar en todo momento la utilización que los órganos judiciales han de hacer de la información. Sólo podrán manipularse los datos estrictamente necesarios para el cumplimiento del fin comentado[2617]. No es exigible que en todo caso se remita toda la historia clínica relativa a un paciente. El juez o magistrado tendrá que determinar qué información necesita atendiendo al caso concreto[2618]. Así lo ha manifestado también la jurisprudencia[2619]. En este sentido, en alguna ocasión se ha subrayado por parte de las agencias de protección de datos la necesidad de que los órganos judiciales especifiquen los documentos que necesitan, para llevar a cabo su función de acuerdo con el principio de finalidad[2620].

[2616] SAN 26 octubre 2005, FJ 4: "Pues bien, a la vista de los citados hechos, el literal del artículo 11.2,d) de la LOPD no es aplicable al presente caso, puesto que dicha excepción al consentimiento del afectado por una cesión de sus datos personales se refiere al supuesto de aquellos datos que se utilizan en un procedimiento judicial cuando han sido requeridos previamente por el Juez en el ejercicio de su funciones, lo que no ocurre en el caso de autos"; SSTS 9 de junio de 2003, FFJJ 2 y 3; 12 de abril de 2005, FJ 2; 17 de noviembre de 2009, FJ 2. DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, pp. 268-269.

[2617] ATELA BILBAO y GARAY ISASI, "Ley 41/2002…", cit., 2004, p. 75; CANTERO RIVAS, "El contenido de la historia…", cit., 2004, p. 391; DE LORENZO Y MONTERO y ESCUDERO GÓNZÁLEZ, "El derecho de acceso…", cit., 2010, p. 1.213. SAN 20 febrero 2008, FJ 5. Dictamen APDCat. CNS 1/2004.

[2618] Sobre la posibilidad de que un juez pueda pedir la historia clínica completa de un paciente, ver el Debate de la Quinta Sesión del Seminario Conjunto sobre Información y Documentación Clínica, celebrado en Madrid los días 22 y 23 de septiembre de 1997, en *Estudios de Derecho Judicial,* nº 7 vol II, 1997, pp. 595-613. El juez o magistrado sólo podrá solicitar la información estrictamente necesaria para la resolución de un problema determinado, y sólo si es absolutamente necesario pedirá toda la documentación sanitaria relativa a una persona concreta. ROMEO CASABONA y CASTELLANO ARROYO, "La Intimidad...", cit., 1993, p. 9, apuntan que "hay que ponderar en cada caso concreto el criterio a seguir".

[2619] STS 4 de diciembre de 2009, FJ 4; AAP de Toledo 7 de julio de 2010, FJ 3, apunta que la aportación completa de una historia clínica resulta "una diligencia desmesurada, que puede vulnerar el derecho constitucional a la intimidad y que no es imprescindible y esencial (…)"; AAP de Murcia 4 de octubre de 2010, FJ 1.

[2620] Resoluciones de la AEPD, R/00840/2007, 22 de agosto de 2007, procedimiento AAPP/00048/2007, FJ. 6 y R/00888/2007, de 21 de septiembre de 2007, procedimiento AAPP/00016/2007, FJ. 4; Recomendación 3, punto

C) En tercer lugar, hay que comentar algo que se ha ido apuntando a lo largo de este apartado. El ordenamiento exige que sean los órganos judiciales los que resuelvan el conflicto que se plantea entre los diferentes bienes jurídicos. Deberán ser los Jueces y Tribunales los que den solución al problema interpretativo que se ha propuesto. Este hecho puede ser criticable desde la perspectiva de las fuentes del derecho[2621].

Cuando los órganos judiciales determinan qué derecho prevalece están fijando los límites de los derechos que se hallan encontrados. En principio, debería ser el poder legislativo, como órgano representante del pueblo, el que determinara dónde se sitúan los límites de los derechos. No deben ser los órganos judiciales quienes de facto establezcan los límites de los derechos fundamentales que aquí se comentan. Es rechazable que la Ley no determine unos criterios mínimos en los que basarse a la hora de concretar el alcance del acceso que pueden tener jueces y tribunales a la historia clínica. Y es que al no haber indicaciones mínimas en la Ley, que fijen la forma en que ha de realizarse la transmisión de la información, se deja al arbitrio de estos funcionarios la determinación del límite del secreto profesional[2622].

No obstante, a falta de una Ley que resuelva la colisión a la que se hace referencia, es indudable que deberán ser los órganos judiciales los que interpreten el ordenamiento y tomen una decisión al respecto[2623]. En todo caso, las decisiones que vayan a tomar deberán ser motivadas. Bien la decisión judicial en la que se exponga la necesidad de traer al proceso cierta información sanitaria, si no la totalidad de la historia clínica, o bien la cédula que llame a declarar al profesional sanitario de turno[2624], deberán exponer los argumentos pertinentes que fundamentan la decisión de llevar a cabo esa actuación. Esta circunstancia hace que estas decisiones puedan ser controlables, de tal forma que la posible arbitrariedad de los órganos

---

tercero, Recomendación de la APDCM, 2/2004, de 30 de julio, sobre Custodia, Archivo y Seguridad de los Datos de Carácter Personal de las Historias Clínicas no Informatizadas: es "necesario que la petición judicial venga motivada y concrete los documentos de la historia clínica que sean precisos conocer para su actuación e investigación, procediéndose por el Centro al envío de una copia de los mismos o a facilitar el acceso dentro del propio Centro"; En relación a la cesión a jueces: pp. 45-46; TRONCOSO REIGADA, *Protección de datos…,* cit., 2008, pp. 98-100; MURILLO DE LA CUEVA, "El Derecho…", cit., 2006, p. 41; la importancia del respeto al principio de finalidad en este punto queda reflejada también en la STEDH, 27 de agosto de 1997, M. S. contra Suecia, Apdos. 39 y siguientes.

[2621] Es importante subrayar que en un proceso judicial en el que entran en juego intereses tanto de pacientes como de médicos, es el juez o magistrado el que tiene que determinar cómo se va a manipular la información relativa al paciente atendiendo a los principios básicos recogidos en el artículo 4º de la LOPD. Hay que subrayar este punto, pues en muchos casos los profesionales sanitarios tienden a solicitar a otros profesionales información sobre el mismo paciente, que les pueda beneficiar en su causa, cosa que de ninguna manera se puede admitir. Es el caso, por ejemplo, de la STSJ de Extremadura, 25 de noviembre de 2002, en la que el tribunal condena a un centro a indemnizar a un paciente por transmitir sus datos médicos a unos médicos que anteriormente trataron a este paciente y que ahora se encontraban en un proceso judicial con el paciente, con el fin de que estos médicos pudiesen obtener más argumentos.

[2622] LEGALIA, *La Protección...*, cit., 2002, p. 143.

[2623] TRONCOSO REIGADA, *Guía de Protección…,* cit., 2004, p. 45.

[2624] Artículo 175 LECrim: "*Las citaciones y emplazamientos se practicarán en la forma establecida para las notificaciones, con las siguientes diferencias:*
-La cédula de citación contendrá:
1.Expresión del Juez o Tribunal que hubiere dictado la resolución, de la fecha de ésta y de la causa en que haya recaído.
2.Los nombres y apellidos de los que debieren ser citados y las señas de sus habitaciones; y si éstas fuesen ignoradas, cualquiera otras circunstancias por las que pueda descubrirse el lugar en que se hallaren.
3.El objeto de la citación.
(...)".

judiciales pueda someterse a juicio. Concretamente, en la mayoría de casos, en la medida en que afectan a los derechos fundamentales, sea la tutela judicial efectiva o la intimidad o el derecho a la autodeterminación informativa, estas decisiones serán revisables[2625].

La necesidad de que sean los órganos judiciales quienes tengan que resolver en cada caso el choque entre bienes jurídicos se ha de subrayar, para poner de manifiesto que en ningún caso serán los propios profesionales sanitarios los que lleven a cabo el juicio de valor. El silencio de la Ley en relación a esta cuestión hace que tengan que ser los órganos judiciales los que lleven a cabo el ejercicio interpretativo necesario para resolver el problema que se plantea. No pueden ser los profesionales sanitarios quienes decidan qué derecho prevalece. La seguridad jurídica ha de ser para los profesionales sanitarios garantizada. Y esta garantía resulta del hecho de que sean los Jueces y Magistrados quienes decidan sobre la necesidad de traer al proceso determinada información sanitaria.

Sin embargo, y teniendo en cuenta que cuando se trata de trasladar información sanitaria se está hablando de una cuestión puramente técnica, estos profesionales tienen que poder aclarar o matizar si parte de la información solicitada por los órganos judiciales es o no necesaria para los fines que se pretenden, de acuerdo con los principios de calidad. Han de articularse las vías necesarias en el proceso para que los órganos judiciales y los profesionales sanitarios puedan comunicarse, de tal forma que a la hora de transmitir la información requerida al proceso los principios de calidad se respeten con el mayor rigor posible.

I.5.4.G. La confrontación entre el derecho a la autodeterminación informativa y el derecho de acceso sobre documentos administrativos en el ámbito sanitario: una propuesta de solución.

I.5.4.G.a. Planteamiento del problema.

La posibilidad de ceder datos sanitarios fuera del ámbito estrictamente médico puede encontrar un argumento favorable en el derecho de acceso sobre los archivos administrativos, entendido como derecho subjetivo[2626]. Podría plantearse la posibilidad de que alegando este derecho un sujeto se haga con información sanitaria, con fines que nada tienen que ver con la salvaguarda de la salud.

El derecho de acceso ha sido reconocido, en el ámbito interno, por la CE[2627], teniendo un desarrollo parcial en diferentes leyes[2628]. En el ámbito de la UE, este derecho se recoge en el

[2625] MURILLO DE LA CUEVA, "El Derecho…", cit., 2006, p. 41.
[2626] EMBID IRUJO, *El Ciudadano y la…,* cit., 1994, p. 89; LUCAS DURÁN, *El acceso a los datos…,* cit., 1997, p. 46; RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 142; PIÑAR MAÑAS, "Transparencia y protección…"; cit., 2010, pp. 83-85, reconoce que el derecho de acceso, más allá de una concreción del principio de transparencia, se erige en un verdadero derecho confrontable con el derecho a la autodeterminación informativa.
[2627] Artículo 105.b) CE: " *La Ley regulará: el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas"*.
[2628] Fundamentalmente, Artículo 37 LPAC y Ley 27/2006, 18 de julio de 2006, por la que se regulan los Derechos de Acceso a la Información, de Participación Pública y de Acceso a la Justicia en materia de Medio Ambiente.

Tratado de Ámsterdam[2629], siendo regulado fundamentalmente por el Reglamento del Parlamento Europeo y el Consejo sobre el acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión[2630]. En el marco del Consejo de Europa ha encontrado regulación en el Convenio sobre el Acceso a los Documentos Públicos, que no ha sido ratificado aún por el Estado español[2631]. Por su parte, en el ámbito autonómico también pueden encontrarse referencias parciales a este respecto[2632].

Reconoce este derecho la posibilidad de que los ciudadanos accedan a los documentos que contiene la Administración en sus ficheros. La finalidad de este ejercicio puede responder a motivos privados, o también a un interés más genérico de controlar la actividad de los poderes públicos y participar en los asuntos de interés general[2633]. Desde esta segunda perspectiva, mediante el acceso la Administración se torna en transparente para los ciudadanos, lo que hace que el derecho repercuta en la profundización democrática del funcionamiento de los poderes públicos[2634]. Resulta evidente que la articulación de mecanismos por los que los ciudadanos pueden controlar la actuación de los poderes públicos constituye una medida que refuerza el carácter democrático y social de un Estado[2635]. El principio de transparencia o/y de publicidad en la actuación de la Administración exige, por lo tanto, que los archivos con los que cuenta sean accesibles para los ciudadanos[2636]. En el caso que aquí interesa, la transparencia de la Administración sanitaria exigiría la posibilidad de que los ciudadanos pudieran acceder a documentos obrantes en sus ficheros.

El problema que plantea el acceso a estos documentos es obvio. En los archivos administrativos es muy fácil encontrarse con datos de carácter personal. En estos casos dicho

[2629] Artículo 255 TCE: "*1. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión, con arreglo a los principios y las condiciones que se establecerán de conformidad con los apartados 2 y 3. (...)*"

[2630] Reglamento 1049/2001, de 30 de mayo de 2001, del Parlamento Europeo y del Consejo, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión. RAMS RAMOS, *El Derecho de Acceso…,* cit., 2008, p. 97.

[2631] Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos, 18 de junio de 2009.

[2632] Artículos 34-37 Ley 10/2001, 13 de julio, de Archivos y Documentos, de Cataluña.

[2633] RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, pp. 199-200.

[2634] CASTELLS ARTECHE, "El Derecho de Acceso…", cit., 1984, pp. 136-137; SÁNCHEZ MORÓN, "El Derecho de Acceso…", cit., 1995, p. 31; FERNÁNDEZ RAMOS, *El Derecho…,* cit., 1997, p. 311; MESTRE DELGADO, *El Derecho de Acceso…,* cit., 1998, p. 50; JIMÉNEZ PLAZA, *El Derecho…,* cit., 2006, p. 15; MARTÍN-RETORTILLO BAQUER, "Prólogo…", cit., 2008, p. 12; TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, p. 39; SOMMERMANN, "La exigencia de una Administración…", cit., 2010, pp. 19-20.

[2635] Artículo 1 CE. STS 30 de marzo de 1999, FJ 3: "El artículo 105.b) de la Constitución dispone que la ley regulará, entre otras materias, <<El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas>>. (…) Refleja una concepción de la información que obra en manos del poder público acorde con los principios inherentes al Estado democrático (en cuanto el acceso a los archivos y registros públicos implica una potestad de participación del ciudadano y facilita el ejercicio de la crítica del poder) y al Estado de derecho (en cuanto dicho acceso constituye un procedimiento indirecto de fiscalizar la sumisión de la Administración a la ley y de permitir con más eficacia el control de su actuación por la jurisdicción contencioso-administrativa)"

[2636] FERNÁNDEZ RAMOS, *El Derecho...,* cit., 1997, p. 329: "Aun cuando el art. 105.b) no menciona la palabra <<derecho>>, es incuestionable que el mandato en él contenido implica el reconocimiento a nivel constitucional de un derecho a la información"; DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, p. 496; GARCÍA MACHO, "El derecho a la información…", cit., 2010, pp. 30-32; LASAGABASTER HERRARTE, "Notas sobre el derecho…", cit., 2010, p. 108.

acceso puede afectar al derecho a la autodeterminación informativa de las personas titulares de esos datos[2637], cuando no a su intimidad. Se puede generar, por lo tanto, un conflicto jurídico entre este derecho y el derecho de acceso de la persona que quiere hacerse con la información contenida en los documentos de la administración alegando, bien un interés particular, o bien el interés común de controlar la actuación del aparato público[2638]. Se tratará de buscar un equilibrio entre los diferentes bienes jurídicos en juego[2639]. Este equilibrio debe encontrarse en las normas.

La normativa aplicable para resolver el conflicto planteado no es clara. Concretamente, desde el punto de vista de la protección de datos, ni las leyes dedicadas a regular esta materia ni las que configuran el régimen jurídico a respetar en el ejercicio del derecho de acceso profundizan con rigor en la cuestión que aquí se plantea[2640]. Ni la LOPD ni el reglamento que la desarrolla hacen mención alguna a esta cuestión. Tampoco las agencias de protección de datos han analizado este conflicto jurídico en profundidad[2641]. La Directiva europea aunque no se refiere de manera expresa al ejercicio del derecho de acceso, reconoce la posibilidad de que una tercera persona tenga acceso a la información concerniente a un sujeto, siempre y cuando demuestre un interés legítimo y no haya un derecho del titular de los datos que prevalezca[2642]. En relación a los datos sanitarios, la Recomendación del Consejo de Europa reguladora de la protección de los datos médicos no se hace eco de este conflicto. Por su parte, la LPAC aporta argumentos más claros a este respecto en su artículo 37, tratando de dar solución al conflicto planteado entre los diferentes bienes jurídicos. Primero, realiza una regulación general del derecho de acceso. Después, se refiere a una serie de supuestos concretos en el que dicho derecho se ve limitado o se sujeta a normas específicas, siendo éste el caso del acceso a documentos que contienen datos sanitarios. Sin embargo, tampoco llega a clarificar en profundidad los criterios a seguir para resolver la colisión entre el derecho de acceso y el derecho a la autodeterminación informativa. Se crea, por lo tanto, en la práctica un vacío legal de relevancia en relación a esta cuestión.

En el supuesto que se estudia se trata de ver si es posible el ejercicio del derecho de acceso sobre ficheros que contienen datos sanitarios. La LPAC recoge una referencia expresa a los archivos que contengan este tipo de información. En esta referencia la Ley se limita a realizar una remisión a las normas que específicamente regulan el acceso a estos datos[2643]. Esta previsión se encuentra con una dificultad: no se reconoce precepto alguno dirigido a solucionar el

[2637] TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, pp. 46-47, se señala que "puede" afectar, debido a que el mero hecho de que en un documento conste un dato de carácter personal no es suficiente para que se entienda afectado el derecho a la autodeterminación de datos. Será necesario que existe un tratamiento de dichos datos.
[2638] GUICHOT, *Datos Personales…,* cit., 2005, pp. 311-312; DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, p. 499; TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, p. 41; GARCÍA MACHO, "Derecho de acceso…", cit., 2008, p. 1.001.
[2639] MONFORT PASTOR, *El Derecho…,* cit., 2004, p. 21; GUICHOT, *Datos Personales…,* cit., 2005, p. 323; PIÑAR MAÑAS, "Transparencia y protección…"; cit., 2010, p. 88.
[2640] GUICHOT, "Acceso a la información…", cit., 2007, p. 435.
[2641] GUICHOT, "Acceso a la información…", cit., 2007, p. 436.
[2642] Artículo 7 Directiva 95/46/CE: "*Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva*"; GUICHOT, *Datos Personales…*, cit., 2005, p. 324.
[2643] Artículo 37.6 LPAC: "*Se regirán por sus disposiciones específicas: b) El acceso a documentos y expedientes que contengan datos sanitarios personales de los pacientes*".

conflicto entre el derecho a la autodeterminación informativa y el derecho de acceso al que ahora se hace referencia en el concreto ámbito de la sanidad. La normativa sanitaria, especialmente la LBAP, regula supuestos específicos de acceso a la historia clínica: por los tribunales, por órganos de inspección, entre otros. Sin embargo, no menciona el derecho de acceso genérico que se reconoce en la LPAC para toda la ciudadanía. Se podría pensar que esta falta de referencia lleva a negar la posibilidad de ejercer el acceso sobre los documentos que contengan datos sanitarios[2644]. Los accesos a estos datos se limitarían a los supuestos previstos en la normativa sanitaria.

No parece que ésta sea una solución aceptable. Ante el vacío legal la solución no debe ser negar absolutamente la posibilidad de ejercer el derecho de acceso sobre los documentos obrantes en la Administración sanitaria que contengan datos de salud. Si así fuera el principio de transparencia quedaría prácticamente anulado en este ámbito. De esta forma, cabe preguntarse si más allá de los accesos concretos reconocidos en la normativa sanitaria se puede alegar un derecho de acceso más genérico con el fin de acceder a documentación médica. Piénsese, por ejemplo, en el supuesto en que un sujeto que padece los síntomas de una enfermedad concreta quiere acceder a documentación sanitaria concerniente a unos vecinos de su barrio que también han padecido dichos síntomas, con el fin de combatir la enfermedad de la manera más efectiva posible o de conocer las posibles causas de la misma; o en el caso en que un ciudadano pretende recabar información, que puede incluir datos sanitarios, sobre el mal funcionamiento de un centro médico concreto basándose en indicios fundados. ¿Es posible alegar en estos supuestos el comentado derecho de acceso? Como se verá a continuación, a pesar de que pueden plantearse dudas en la solución a esta cuestión, no resulta descabellado dar una respuesta en sentido afirmativo. Se entiende que frente a la falta de disposiciones específicas cabe acudir al régimen general que recoge el artículo 37 LPAC para extraer los criterios que han de seguirse para resolver la convivencia entre los derechos afectados.

En primer lugar, reconoce este precepto que el derecho de acceso puede ejercerse sobre cualquier archivo o registro administrativo, cualquiera que sea su formato, siempre y cuando se refiera a un procedimiento terminado. En segundo lugar, niega la posibilidad de acceder a los datos que afectan a la intimidad de las personas. Y por último señala que el tercero que demuestre un interés legítimo y directo podrá tener acceso a los datos nominativos que no afecten a la intimidad de las personas y que no se refieran a un procedimiento sancionador[2645]. Esta regulación ha sido criticada debido a la ambigüedad de sus términos y a que no constituye

[2644] RAMS RAMOS, *El Derecho de Acceso…,* cit., 2008, p. 534.

[2645] Artículo 37 LPAC: "*1. Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud.*
2. El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a éstas, que, en el esupuesto de observar que tales datos figuran incompletos o inexactos, podrán exigir que sean rectificados o completados, salvo que figuren en expedientes caducados por el transcurso del tiempo, conforme a los plazos máximos que determinen los diferentes procedimientos, de los que no pueda derivarse efecto sustantivo alguno.
3. "El acceso a los documentos de carácter nominativo que sin incluir otros datos pertenecientes a la intimidad de las personas figuren en los procedimientos de aplicación del derecho, salvo los de carácter sancionador o disciplinario, y que, en consideración a su contenido, puedan hacerse valer para el ejercicio de los derechos de los ciudadanos, podrá ser ejercido, además de por sus titulares, por terceros que acrediten un interés legítimo y directo".

un régimen especialmente favorable al ejercicio del derecho de acceso[2646]. Del análisis del precepto que se acaba de citar deberán desprenderse los criterios necesarios para resolver el enfrentamiento de derechos arriba expuesto.

I.5.4.G.b. En torno a la posibilidad de argumentar el derecho de acceso sobre las historias clínicas

Como punto de partida será necesario preguntarse si es posible ejercer el derecho de acceso sobre una historia clínica. La relevancia del análisis del derecho de acceso deriva de la consideración de la historia clínica contenida en los centros sanitarios públicos como documento administrativo. La normativa administrativa reconoce la posibilidad de ejercer el derecho de acceso sobre los archivos, registros y documentos administrativos que obren en los expedientes relativos a procedimientos terminados en la fecha de la solicitud de acceso[2647]. Una interpretación especialmente estricta de este precepto podría limitar, sino negar, la posibilidad de ejercer dicho derecho sobre las historias clínicas. No obstante, puede plantearse una interpretación amplia de la letra de la norma, que favorezca la posibilidad de ejercer el acceso sobre los documentos comentados.

La defensa de esta interpretación amplia comienza, teniendo en cuenta que los archivos y registros están constituidos por documentos[2648], por aclarar qué se entiende por documento[2649]. Se trata, según el propio ordenamiento administrativo, de "*toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos. Se excluyen los ejemplares no originales de ediciones*"[2650]. Ha señalado la doctrina que los documentos integran tres elementos: el soporte, el mensaje y la incorporación del mensaje en dicho soporte[2651]. Partiendo de este concepto se deduce, tal como hacen las leyes, que los documentos públicos administrativos son aquéllos que son emitidos por cualquier Administración[2652]. Lo mismo resulta de la normativa autonómica[2653] y del Convenio del Consejo de Europa, refiriéndose este último a "toda la

[2646] SÁNCHEZ MORÓN, "El Derecho de Acceso…", cit., 1995, p. 38; POMED SÁNCHEZ, "El acceso a los archivos…", cit., 1997, p. 466; FERNÁNDEZ RAMOS, *El Derecho de Acceso…,* cit., 1997, pp. 377-378; GUICHOT, "El nuevo Derecho Europeo…", cit., 2003, p. 284; GUICHOT, *Datos Personales…,* cit., 2005, p. 336; GUICHOT, *Publicidad y Privacidad…*, cit., 2009, p. 200; GARCÍA MACHO, "El derecho a la información…", cit., 2010, p. 43; PIÑAR MAÑAS, "Transparencia y protección…", cit., 2010, p. 98; TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, pp. 712-713.
[2647] Artículo 37.1 LPAC.
[2648] FERNÁNDEZ RAMOS, *El Derecho…,* cit., 1997, p. 418.
[2649] MONFORT PASTOR, *El Derecho…,* cit., 2004, p. 127.
[2650] Artículo 49.1 Ley 16/1985, 25 de junio de 1985, del Patrimonio Histórico Español.
[2651] SENDÍN GARCÍA, "El documento…", cit., 2009, p. 21.
[2652] Artículo 46.4 LPAC: "*Tienen la consideración de documento público administrativo los documentos válidamente emitidos por los órganos de las Administraciones Públicas*".
[2653] Artículo 6 Ley 10/2001, 13 de julio de Archivos y Documentos, de Cataluña: "*1. A efectos de la presente Ley, son documentos públicos los que producen o reciben en el ejercicio de sus funciones: a. El Presidente, el Gobierno y la Administración de la Generalidad; b. El Parlamento de Cataluña, el Síndic de Greuges, la Sindicatura de Cuentas y el Consejo Consultivo y todas las demás instituciones de la Generalidad no dependientes de su Administración; c. Las Administraciones Locales; d. Los órganos con sede en Cataluña de la Administración General y de los poderes del Estado; e. Los órganos con sede en Cataluña de la Unión Europea y de instituciones públicas internacionales; f. Las Entidades de Derecho Público o Privado vinculadas a cualquiera de las administraciones públicas o que dependen de ellas; g. Las empresas y las instituciones privadas concesionarias de servicios públicos, en lo que se refiere a estas*

información registrada de cualquier forma, elaborada o recibida, y en posesión de las autoridades públicas"[2654]. Se entiende que alcanzan a todos los documentos de los que disponen las administraciones, no sólo las territoriales[2655]. La interpretación que se maneja de este concepto es, por lo tanto, amplia[2656]. Partiendo de estas definiciones se podría afirmar que las historias clínicas que se encuentran en los centros públicos se integran en esta categoría[2657]. Se trata de documentos que, además, se ubican en archivos organizados en base a criterios previamente definidos[2658].

Además de exigir que se trate de documentos obrantes en archivos administrativos, la normativa estatal requiere que el ejercicio del acceso se lleve a cabo, sólo, sobre la documentación contenida en expedientes relativos a procedimientos ya terminados. El ordenamiento ha definido el concepto de expediente como el conjunto ordenado de documentos de la Administración referidos a un procedimiento concreto, que finalizará con una resolución[2659]. Teniendo en cuenta esta definición y que, además, el expediente ha de referirse a un procedimiento terminado, la aplicabilidad de esta regulación a las historias clínicas podría ser complicada. La consideración de los procesos asistenciales que se reflejan en una historia clínica como procedimientos ya terminados podría ser dudosa[2660]. Sin embargo, atendiendo a la definición amplia que se pretende dar desde diferentes instancias al concepto de documento y ante el alcance que en la actualidad se está intentando dar al derecho de acceso[2661], no es descartable que este derecho pueda ejercerse en el ámbito sanitario sobre las historias clínicas. En alguna ocasión la propia doctrina ha considerado técnicamente la historia clínica como un

concesiones; h. Los fedatarios y los registros públicos; i. Las corporaciones privadas de Derecho Público; j. Las personas y las entidades privadas que ejercen funciones públicas, en lo que se refiere a estas funciones; k. Cualquier entidad pública o entidad dependiente de una entidad pública no incluida en las letras precedentes.
2. Se consideran incluidos en la enumeración del apartado 1 los documentos producidos o recibidos por las personas físicas que ocupan cargos políticos en instituciones públicas, siempre que estos documentos tengan relación con las funciones administrativas o políticas propias del cargo".

[2654] Artículo 1.2.b) Convenio del Consejo de Europa sobre el acceso a los documentos públicos, 18 de junio de 2009.

[2655] JIMÉNEZ PLAZA, *El Derecho…,* cit., 2006, pp. 47-48.

[2656] FERNÁNDEZ RAMOS, *El Derecho de Acceso…*, cit., 1997, pp. 422-423; MESTRE DELGADO, *El Derecho de Acceso…,* cit., 1998, p. 135; SÁNCHEZ MORÓN, *Derecho Administrativo…,* 2007, p. 456.

[2657] DE MIGUEL SÁNCHEZ, *Secreto Médico…,* cit., 2002, p. 153.

[2658] Artículo 59.1, Ley 16/1985, 25 de junio de 1985, del Patrimonio Histórico Español: "*Son archivos los conjuntos orgánicos de documentos, o la reunión de varios de ellos, reunidos por las personas jurídicas, públicas o privadas, en el ejercicio de sus actividades, al servicio de su utilización para la investigación, la cultura, la información y la gestión administrativa.*
Asimismo, se entienden por archivos las instituciones culturales donde se reúnen, conservan, ordenan y difunden para los fines anteriormente mencionados dichos conjuntos orgánicos". RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 240; SENDÍN GARCÍA, "El expediente administrativo…", cit., 2009, p. 83.

[2659] Artículo 164 RD 2568/1986, 28 de noviembre de 1986, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales: "*Constituye expediente el conjunto ordenado de documentos y actuaciones que sirven de antecedentes y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla*". RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 410.

[2660] Artículo 14.1 LBAP: "*LA historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro*".

[2661] RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 227.

expediente administrativo personal, que si bien no tiene como fin la adopción de una resolución, se dirige a recopilar datos concernientes a las personas[2662].

Se puede traer como argumento favorable a esta interpretación, el hecho de que en materia medioambiental la normativa no exija que los documentos se refieran a un expediente correspondiente a un procedimiento ya terminado, y que, aunque no reconoce expresamente la posibilidad de acceder a las historias clínicas, menciona la facultad de acceder a los datos de salud de los ciudadanos[2663]. Hay que tener en cuenta también que la regulación llevada a cabo en la LPAC contradice lo dispuesto en la Constitución, que se refiere simplemente "a los archivos y registros administrativos", sin mayor limitación[2664]. Como acertadamente ha considerado parte de la doctrina, la referencia a los procedimientos terminados no ha de negar la posibilidad de ejercer el derecho de acceso sobre otros documentos que puedan encontrarse en ficheros públicos[2665]. Esta perspectiva amplia se ha apoyado también, en algún caso, en el derecho comparado, al entender que en el momento en que una información es empleada por la Administración adquiere relevancia pública, erigiéndose en potencialmente accesible[2666].

No puede olvidarse que el derecho de acceso constituye una herramienta fundamental para que el principio de transparencia en la Administración no se convierta en un mero principio programático, sin eficacia jurídica, y que el acceso a los datos contenidos en las historias clínicas puede resultar fundamental, para poder controlar la actividad de la Administración sanitaria.

I.5.4.G.c. El derecho a la autodeterminación informativa como límite al derecho de acceso en el ámbito sanitario.

Tras justificar, aunque con cierta prudencia, la posibilidad de ejercer el derecho de acceso sobre los documentos obrantes en la Administración sanitaria, entre los que están las historias clínicas, es necesario profundizar en la consideración que la Ley realiza de la intimidad y la autodeterminación informativa como límites al ejercicio del citado derecho. La LPAC limita de forma distinta el derecho de acceso dependiendo de si los datos que se quieren obtener afectan

[2662] GARCÍA SENDÍN, "El expediente administrativo…", cit., 2009, p. 84.
[2663] Artículo 1.1 Ley 27/2006, 18 de julio de 2006, por la que se regulan los Derechos de Acceso a la Información, de Participación Pública y de Acceso a la Justicia en materia de Medio Ambiente: "*Esta Ley tiene por objeto los siguientes derechos: a) A acceder a la información ambiental que obre en poder de las autoridades públicas o en el de otros sujetos que la posean en su nombre (…)*"; Artículo 2 Ley 27/2006, 18 de julio de 2006, por la que se regulan los Derechos de Acceso a la Información, de Participación Pública y de Acceso a la Justicia en Materia de Medio Ambiente.: "*A los efectos de esta Ley se entenderá por: 3. Información ambiental: toda información en forma escrita, visual, sonora, electrónica o en cualquier otra forma que verse sobre las siguientes materias: f) El estado de salud y seguridad de las personas, incluida, en su caso, la contaminación de la cadena alimentaria, condiciones de vida humana, bienes del patrimonio histórico, cultural y artístico y construcciones, cuando se vean o puedan verse afectados por el estado de los elementos del medio ambiente citados en la letra a o, a través de esos elementos, por cualquiera de los extremos citados en las letras b y c*".
[2664] LUCAS DURÁN, *El Acceso a los Datos…,* cit., 1997, pp. 77-78; RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 413..
[2665] SÁNCHEZ MORÓN, *Derecho Administrativo…,* 2007, p. 457: "En cualquier caso, la alusión a los procedimientos terminados no limita el acceso a documentos que no se integran en un expediente formalizado, sino que forman parte de otras actuaciones y que obren en poder de la Administración"; RAMS RAMOS, *El Derecho de acceso…,* cit., 2008, p. 421.
[2666] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 172.

a la intimidad o a la "privacidad"[2667], término empleado en la LORTAD para designar el derecho a la autodeterminación informativa[2668]. En el primer supuesto el acceso a la información no está permitido. El derecho de acceso cede cuando choca contra la intimidad, otorgando a este último derecho carácter absoluto. En el segundo supuesto, cuando afecte a los datos nominativos, el acceso estará sujeto a una serie de condiciones.

La interpretación de esta norma no es nada sencilla. Definir lo que es íntimo y lo que simplemente consiste en datos nominativos resulta complicado[2669]. De hecho, esta distinción entre datos íntimos y nominativos no se ha seguido o mantenido en posteriores normas dirigidas a regular el derecho de acceso en otros ámbitos de actuación de la Administración. Es el caso de la ya mentada Ley que regula el acceso a la información en materia de medio ambiente[2670].

De inicio, la LPAC niega la posibilidad de ejercer el derecho de acceso sobre las informaciones que afectan a la intimidad de las personas[2671]. Ya se ha comentado la dificultad de determinar el contenido de un concepto tan subjetivo como el de intimidad[2672]. En principio podría interpretarse en el sentido clásico del mismo, como ámbito que se pretende reservar ante las demás personas y que se quiere proteger con especial celo[2673]. Atendiendo a esta definición la consideración de los datos de salud como íntimos no plantea de inicio ninguna dificultad. El reconocimiento del derecho a la intimidad en el ámbito sanitario se realiza de manera expresa tanto en normas[2674] como en la jurisprudencia[2675], y en algún caso se ha llegado a afirmar

[2667] GUICHOT, *Datos Personales…,* cit., 2005, p. 338.
[2668] STSJ de Cataluña de 26 de noviembre de 1999, FJ 2.
[2669] RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 262.
[2670] Artículo 13 Ley 27/2006, de 18 de julio, por la que se regulan los Derechos de Acceso a la Información, de Participación Pública y de Acceso a la Justicia en Materia de Medio Ambiente: "*2.Las solicitudes de información ambiental podrán denegarse si la revelación de la información solicitada puede afectar negativamente a cualquiera de los extremos que se enumeran a continuación: f)Al carácter confidencial de los datos personales, tal y como se regulan en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siempre y cuando la persona interesada a quien conciernan no haya consentido en su tratamiento o revelación (…)*
4.Los motivos de denegación mencionados en este artículo deberán interpretarse de manera restrictiva. Para ello, se ponderará en cada caso concreto el interés público atendido con la divulgación de una información con el interés atendido con su denegación.
5.Las autoridades públicas no podrán en ningún caso ampararse en los motivos previstos en el apartado 2, letras a), d), f), g) y h) de este artículo, para denegar una solicitud de información relativa a emisiones en el medio ambiente". CUBERO MARCOS, "Excepciones al…", cit., 2007. p. 157. CASADO CASADO, "El Derecho de acceso…", cit., 2009, p. 312.
[2671] Artículo 37.2 LPAC. EMBID IRUJO, *El Ciudadano y la Administración…,* cit., 1994, p. 97; MESTRE DELGADO, *El Derecho de Acceso…,* cit., 1998, pp 159-161; DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, pp. 541-542.
[2672] FERNÁNDEZ RAMOS, *El Derecho…*, cit., 1997, p. 488: pone de manifiesto la dificultad de definir y dar contenido a este concepto.
[2673] MONFORT PASTOR, *El Derecho…,* cit., 2004, p. 141; REBOLLO DELGADO, *El Derecho Fundamental…*, cit., 2005, p. 73. STC 30 noviembre de 2000, FJ 6: "La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad"; STC 23 de marzo de 2009, FJ 2: "el derecho a la intimidad personal garantizado por el art. 18.1 CE, estrechamente vinculado con el respeto a la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana".
[2674] Artículo 7 LBAP: "*El derecho a la intimidad- 1.Toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que pueda acceder a ellos sin previa autorización amparada por la Ley*".

expresamente que dicha información pertenece al ámbito de la intimidad[2676]. Vinculando el concepto de intimidad con la normativa de protección de datos se puede llegar a la misma conclusión. No sería descabellado integrar los datos sensibles en el ámbito de lo íntimo[2677]. Y no hay que olvidar que los datos de salud entran en este grupo. Así, teniendo en cuenta que los datos sanitarios son considerados por la LOPD datos sensibles, y partiendo de que esta información es íntima, se podría negar aplicando estrictamente la LPAC la posibilidad de ejercer el derecho de acceso sobre los citados datos[2678].

No se entiende aquí que la solución a la cuestión que se analiza pase por la prohibición absoluta al ejercicio del acceso sobre este tipo de información. Ya se ha apuntado más arriba el problema que plantean los datos considerados como sensibles[2679]. La sensibilidad depende más de las circunstancias que rodean a su manipulación que de la propia naturaleza de los mismos. Es por ello por lo que hacer una enumeración de la información que se considera íntima resulta especialmente complejo. Esta interpretación es válida tanto para la normativa que regula la protección de los datos de carácter personal como para la dirigida a ordenar el procedimiento administrativo común. Puede partirse, por lo tanto, de una interpretación más flexible de lo que tiene que entenderse por datos sensibles o intimidad. Cualquier dato puede ser sensible dependiendo de las circunstancias en las que se manipule. Así, cuando se habla de intimidad no se hace referencia a una serie de datos, sino a las circunstancias que rodean a la manipulación de la información que se pretende tratar y cómo afecta la manipulación de esa información en la dignidad de la persona. Siendo esto así, los datos sanitarios no siempre han de ser considerados como sensibles o íntimos y sujetarse a una protección absoluta. Partiendo de esta afirmación puede llegar a reconocerse que es posible argumentar el derecho de acceso que se comenta para acceder a la documentación sanitaria. El que se facilite o no ese acceso dependerá de las circunstancias que rodeen al caso concreto,

Se interpreta que la resolución de la colisión entre derechos planteado se realizará atendiendo a las circunstancias de cada caso, a los intereses concretos que entran en juego[2680]. Esta línea interpretativa encuentra fundamento en diferentes fuentes. Tiene base, sobre todo, en la esfera internacional. El supervisor europeo expresamente ha establecido que los datos que son objeto en las leyes de una especial protección pueden ser también manipulados, sin necesidad de recabar el consentimiento del titular, incluso a efectos del ejercicio del derecho de acceso[2681]. También desde los tribunales parece haberse seguido la misma línea interpretativa. En un supuesto en que se limitaba el derecho de acceso a unos archivos de las instituciones de

[2675] STS 25 febrero de 2002, FJ 3

[2676] STC 23 de marzo de 2009, FJ 2: "Dentro de ese ámbito propio y reservado frente a la acción y el conocimiento de los demás que preserva el derecho a la intimidad contenido en el art. 18.1 CE, se comprende, sin duda, la información relativa a la salud física o psíquica de una persona (…)"..

[2677] GUICHOT, *Datos Personales…,* cit., 2005, p. 339-340; DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, pp. 538-539. GUICHOT, *Publicidad y Privacidad…*, cit., 2009, p. 205.

[2678] FERNÁNDEZ RAMOS, *El Derecho...*, cit., 1997, pp. 514-516, parece llegar a dicha conclusión; TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, p. 79.

[2679] GUICHOT, *Publicidad y Privacidad…*, cit., 2009, p. 216.

[2680] GUICHOT, "Acceso a la información…", cit., 2007, p. 440.

[2681] Apartado 3.4.4 Supervisor Europeo de Protección de Datos, *Public acces to documents and data protection*, Background Paper Series, nº 1, julio de 2005.

la UE argumentando la confidencialidad de la información que contenían, los tribunales concluyeron que dicha limitación debía analizarse caso por caso. Si bien es verdad que en algún momento la decisión de los tribunales hacía una referencia expresa a los datos sensibles, considerados como tales en el Reglamento del Parlamento europeo y el Consejo que regula el tratamiento de los datos de carácter personal contenidos en las instituciones y los organismos comunitarios[2682], parece que el argumento de fondo se basaba en el análisis de las circunstancias de cada supuesto[2683]. Esta visión se refuerza por el hecho de que estos tribunales hacen un llamamiento a que las excepciones al derecho de acceso sean interpretadas de forma restrictiva[2684]. También el Grupo de Trabajo creado en el marco de la Directiva europea sobre protección de datos de carácter personal sigue el mismo criterio. Señala que a la hora de limitar el acceso a los ficheros públicos habrá que ver, en cada caso, si el acceso que se pretende causa un perjuicio a la persona titular de los datos que se quieren conocer[2685]. Del articulado del Convenio del Consejo de Europa resulta la misma interpretación. Dispone que la intimidad "puede" ser un límite al ejercicio del derecho de acceso[2686]. Sin embargo, el acceso sólo será rechazado si en un caso particular se entiende que puede dañar la intimidad[2687]. El análisis, por lo tanto, deberá hacerse atendiendo a cada supuesto. Esta afirmación ha sido puesta de manifiesto también por la doctrina[2688]. En esta línea, la doctrina ha apuntado también en alguna ocasión la posibilidad de ejercer el derecho de acceso sobre los datos que de inicio son considerados como íntimos[2689].

[2682] Artículo 10 Reglamento 45/2001, del Parlamento Europeo y del Consejo de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos: "*Se prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad*".

[2683] CASADO CASADO, "El Derecho de acceso…", cit., 2009, pp. 314-315, en referencia a la Sentencia del Tribunal de Primera Instancia 8 de noviembre de 2007, Bavarian Lager c. Comisión. Esta sentencia ha sido anulada posteriormente por STSJCE, 29 de junio de 2010, Comisión Europea c. The Bavarian Lager, si bien esta decisión no afecta al argumento que aquí se ha prestado, en el sentido de que la ponderación entre los derechos en juego se realiza caso por caso.

[2684] GARCÍA MACHO, "El derecho a la información…", cit., 2010, pp. 37-38.

[2685] Dictamen del Grupo de Trabajo del artículo 29, 3/99, sobre protección de datos, relativo a la información en el sector público y protección de datos personales, 3 de mayo de 1999,. Apartado 4.f) Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 5/2001, sobre el Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo a raíz del proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, 17 de mayo de 2001,.

[2686] Artículo 3.1 Convenio del Consejo de Europa sobre el acceso a los documentos públicos, 18 de junio de 2009: "*Cada parte puede limitar el derecho del acceso a los documentos públicos. Los límites deberán estar previstos por una ley, ser necesarios en una sociedad democrática y tener como objetivo la protección de: (...) f) la intimidad y otros intereses privados legítimos*".

[2687] Artículo 3.2 Convenio del Consejo de Europa sobre el acceso a los documentos públicos, 18 de junio de 2009: "*El acceso a la información contenida en un documento oficial puede ser rechazado si puede o probablemente pueda dañar los intereses mencionados en el párrafo 1, a menos que haya un interés público que prevalezca en dicha revelación*".

[2688] PIÑAR MAÑAS, "Transparencia y protección…"; cit., 2010, p. 90, ha señalado la necesidad de que la confrontación entre el derecho de acceso y la autodeterminación informativa sea analizada caso por caso.

[2689] FERNÁNDEZ RAMOS, *El Derecho de Acceso...*, cit., 1997, p. 498; LUCAS DURÁN, *El Acceso a los Datos…,* cit., 1997, pp. 246-247, también parece apuntar en esta línea al referirse al acceso a los datos en poder de la Administración tributaria, al señalar que cuando existe una causa justificativa suficiente el derecho de acceso puede ejercerse; FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 178; GARCÍA MACHO, "Derecho de acceso…", cit., 2008, pp. 1.001-1.002.

Teniendo en cuenta, por lo tanto, que no se partirá de distinciones preestablecidas entre datos a los que se puede acceder y a los que no, lo que habrá que analizar será cuáles son los intereses concretos que chocan en cada caso. El acceso a los datos sanitarios será posible dependiendo del interés que se alegue para ello. En referencia a este concepto de interés, la LPAC, cuando regula el acceso a los datos nominativos, dispone que para poder ejercer el acceso a dicha información deberá alegarse un "interés legítimo y directo"[2690]. Será necesario un interés lo suficientemente relevante como para que el derecho a la autodeterminación informativa decaiga a favor del derecho de acceso[2691].

Este concepto de interés legítimo y directo ha sido muy discutido en la doctrina[2692] y por los tribunales[2693]. Se ha considerado en numerosas ocasiones que la exigencia de dicho interés limita en exceso el derecho de acceso[2694]. En concreto, añadir el requisito de que el interés haya de ser directo, además de legítimo, parece establecer un nivel de exigencia muy alto[2695]. En contraposición a esta perspectiva tan restrictiva que aportaría una lectura literal de la Ley se ha propuesto, fundamentalmente por la doctrina, la necesidad de otorgar un sentido amplio al concepto que se analiza, sin que el empleo del término "directo" lleve a una restricción excesiva del sujeto activo facultado para ejercer el derecho de acceso sobre estos datos[2696]. Partiendo, otra vez, de fuentes internacionales se ha interpretado que de partida, para ejercer el derecho de acceso sobre los documentos administrativos no es necesario mostrar un interés específico[2697].

[2690] Artículo 37.3 LPAC.

[2691] FERNÁNDEZ SALMERÓN, *La Protección...*, cit., 2003, p. 178, niega que "todo dato sensible constituya un límite insuperable para el ejercicio del Derecho de acceso a los documentos administrativos de conformidad con el artículo 37.2 LRJPC" y entiende que, "al contrario, no cualquier demanda de acceso deba prosperar frente a informaciones no consideradas sensibles desde la óptica de la protección de los datos personales". Señala este autor, refiriéndose al conflicto entre el derecho al acceso y el derecho a la intimidad que recoge el artículo 37.2, "que resulta evidente que la confrontación entre derechos no puede resolverse en un ordenamiento coherente y progresivo mediante la absoluta y sistemática prevalencia de uno de ellos".

[2692] EMBID IRUJO, *El Ciudadano y la Administración…,* cit., 1994, p. 101; GUICHOT, *Datos Personales…,* cit., 2005, p. 342.

[2693] STC 23 de marzo de 2004, FJ 4; entiende el Tribunal Constitucional por interés legítimo "la titularidad potencial de una ventaja o de una utilidad jurídica, no necesariamente de contenido patrimonial, por parte de quien ejercita la pretensión, y que se materializaría de prosperar ésta. Luego, para que exista interés legítimo, la actuación impugnada debe repercutir de manera clara y suficiente en la esfera jurídica de quien acude al proceso"; STS 22 de mayo de 1996, FJ 5: "La cualidad de interesado ha de reconocerse (…) <<en quien, persona física o jurídica, manifiesta y acredita, al menos "prima facie", ante el Órgano judicial, una conexión de carácter concreto y singular bien con el objeto mismo del proceso (…) bien con alguno de los actos procesales a través de los que aquél se ha desarrollado y que están documentados en autos>>"; STS 6 de junio de 2005, FJ 7; STSJ de Castilla y León 1 de marzo de 2006, FJ 4: se entiende por interés legítimo y directo "la posibilidad de que el acceso a los documentos depare a quien lo pretende un beneficio o provecho o le sirve para evitar o disminuir un perjuicio"

[2694] SÁNCHEZ MORÓN, "El Derecho de Acceso…", cit., 1995, p. 39; MESEGUER YEBRA, *El Derecho…,* cit., 2000, pp. 9-10; RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, pp. 366-367. Esta exigencia podría ser, incluso, contraria a la previsión constitucional, que reconoce el derecho de acceso a los "ciudadanos" MESTRE DELGADO, *El Derecho de Acceso…,* cit., 1998, p. 189; TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, p. 52.

[2695] STSJ de Madrid, 12 de abril del 2000, FJ 2; STSJ de Andalucía, 24 de febrero de 2003, FJ 2: interpretan que el concepto "directo" es más restrictivo que el de "legítimo". FERNÁNDEZ RAMOS, *El Derecho de Acceso…,* cit., 1997, p. 502: ha apoyado la posibilidad de que se entienda que es suficiente con la presencia o alegación del interés legítimo.

[2696] MONFORT PASTOR, *El Derecho…,* cit., 2004, pp. 145-147; RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 374.

[2697] CASADO CASADO, "El Derecho de acceso…", cit., 2009, pp. 313-314, en referencia a la Sentencia del Tribunal de Primera Instancia 8 de noviembre de 2007, Bavarian Lager c. Comisión, subraya la falta de necesidad de demostrar

Este interés sólo será necesario cuando el acceso afecte a la intimidad del titular de los datos. En este caso será necesario ponderar los intereses en juego, supuesto por supuesto, para concluir si es posible ejercer el acceso o no[2698]. El derecho de acceso a los datos nominativos no se limitaría a quienes demostraran un interés legítimo y directo, sino que se abriría a todos los ciudadanos. El límite se aplicaría si, una vez aplicado el principio de proporcionalidad, en un caso determinado se concluyera que ese acceso afecta de manera contraria al Derecho a la intimidad o autodeterminación informativa del titular de los datos[2699].

En lo referente a la protección de los datos sanitarios, la aplicación del criterio que se acaba de exponer llevaría a la siguiente conclusión. Los datos de salud son, inicialmente, merecedores de una protección especial, por lo que el acceso a los mismos resulta difícil sin el consentimiento del titular. Los motivos que pueden justificar dicho ejercicio sin el consentimiento del titular deberán responder a intereses de suficiente entidad. En principio, ya se ha visto que la normativa sanitaria y de protección de datos reconocen una serie de finalidades que justifican el acceso a la información sanitaria: defensa de la salud pública o de la salud de terceras personas, intereses colectivos como la actividad inspectora de la administración tributaria, etc. Sin embargo, cabe preguntar aquí si, más allá de estos intereses particulares, puede alegarse en atención a los argumentos dados un interés genérico al derecho de acceso a los datos sanitarios con el fin de controlar la actividad y funcionamiento de la Administración sanitaria o perseguir otro interés de carácter general, como puede ser el citado acceso a información de relevancia medioambiental.

Es evidente, e incluso comprensible, la duda que se plantea en torno a la posibilidad de limitar un derecho fundamental, como el derecho a la autodeterminación informativa, en base a un bien jurídico tan ambiguo como el bien común[2700]. Aquí sí se estaría añadiendo un argumento nuevo que limitaría el citado derecho fundamental. Sin embargo, se entiende que en casos en que la finalidad de controlar la actividad de la Administración o de salvaguardar otro bien de

---

un interés determinado para poder acceder a documentos de la Administración, en este caso de las instituciones de la Unión Europea. En la misma línea, Apartados 2.4.2 y 4.2.2. *Public acces to documents and data protection*, Supervisor Europeo de Protección de Datos, Background Paper Series, nº 1, julio de 2005: sigue el mismo criterio de atender a cada caso para que, en aplicación del principio de proporcionalidad, se concluya si prevalece el derecho de acceso o el derecho a la intimidad. De la normativa europea puede deducirse el mismo criterio: Artículo 2.1 Reglamento 1049/2001, del Parlamento europeo y del Consejo sobre el derecho de acceso del público a los documentos del Parlamento Europeo y del Consejo: "*Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tiene derecho a acceder a los documentos de las instituciones, con arreglo a los principios, condiciones y límites que se definen en el presente Reglamento*"; Artículo 4.1 Reglamento 1049/2001, del Parlamento europeo y del Consejo sobre el derecho de acceso del público a los documentos del Parlamento Europeo y del Consejo: "*Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de: (...) b) La intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales*". No se requiere en ningún momento demostrar un interés concreto para acceder a la información que consta en los archivos de esas instituciones. Otra cosa será que el derecho de acceso pueda verse limitado porque el conocimiento de dichos datos causa un perjuicio a la intimidad de determinadas personas. GUICHOT, "El nuevo Derecho Europeo…", cit., 2003, p. 298; RAMS RAMOS, *El Derecho de Acceso…*, cit., 2008, p. 104.

[2698] STJUE, 29 de junio de 2010, Comisión Europea v. The Bavarian Lager, FFJJ 75-79, apunta que es necesario que quien quiere ejercer el derecho de acceso a unos datos de carácter personal demuestre un interés concreto para que sea posible la ponderación ente los intereses en juego.

[2699] GUICHOT, "Acceso a la información…", cit., 2007, p. 419; TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, pp. 749-750.

[2700] MONFORT PASTOR, *El Derecho…*, cit., 2004, pp. 41-42.

interés general es especialmente clara puede llegar a limitarse, según las circunstancias, el derecho a la autodeterminación informativa. La solución deberá buscarse caso por caso. Más arriba se han puesto ejemplos concretos que podrían llevar a aplicar la excepción que ahora se analiza. Se citaba el caso en que se quiere tener acceso a la información contenida en una historia clínica, con el fin de conocer los efectos dañinos que se intuye puede estar causando una empresa determinada, o el supuesto en que se pretende acceder a determinada información porque se tiene fundada sospecha de que el funcionamiento de un centro sanitario no es correcto en relación a unos hechos que incluso pueden llegar a afectar al propio solicitante.

Ante la dificultad de determinar en cada supuesto cuándo existe el interés público que podría justificar el acceso a la información sanitaria, resulta especialmente importante subrayar la necesidad de que, cuando se plantee el enfrentamiento de derechos que se comenta, se lleve a cabo un ejercicio de ponderación en el que se valore la cualidad de los datos a los que se pretende acceder, es decir, ver en qué medida afectan a la intimidad de las personas, y se analice de qué manera estos datos de carácter personal pueden ayudar al ejercicio del bien común argumentado[2701]. En este sentido, habrá que articular los medios necesarios para que los diferentes derechos en juego puedan verse satisfechos en la mayor medida posible.

Es necesario que cuando se ejerce el derecho de acceso, incluso cuando afecte a datos sensibles, la respuesta inmediata no sea la negación del derecho. El principal instrumento a valorar a la hora de ponderar la colisión entre la intimidad o la autodeterminación informativa y el derecho de acceso lo constituirá la disociación. Deberá analizarse si se puede satisfacer el acceso ocultando la identidad de los sujetos afectados en el documento administrativo, pues en ese caso deberá ejecutarse el proceso de disociación[2702]. La voluntad de cualquier ciudadano de acceder a información sanitaria con objetivos que responden a un interés general muchas veces puede verse satisfecha con el acceso a datos disociados. A esta fórmula se ha hecho referencia, por ejemplo, en recientes pronunciamientos del TJUE. Este Tribunal ha tratado el supuesto en que una Administración alemana publica, en cumplimiento de la normativa interna, información de contenido económico relativa a determinadas personas, incluyendo su identidad. Esta circunstancia enfrentaba directamente el derecho a la autodeterminación informativa y el principio de transparencia. Ante este hecho, ha subrayado el Tribunal que si bien la publicación de los datos está justificada en aras de una mayor transparencia, para hacer efectivo este principio no es necesario sacar a la luz los nombres de los titulares de los datos. Se aboga por la disociación de la información a publicar por la Administración, para encontrar así un mayor equilibrio entre la transparencia en la actividad administrativa y los intereses de aquéllos sobre los que se informa, en tanto en cuanto la información publicada no se vincula a determinadas personas[2703]. Con esto se quiere poner de manifiesto que el responsable que deba hacer efectivo el derecho de acceso tendrá la obligación de tomar en consideración la posibilidad de disociar los datos, sin que el mero hecho de que la intimidad de una persona pueda verse afectada lleve a negar automáticamente el acceso.

[2701] GUICHOT, *Datos Personales...,* cit., 2005, pp. 345-346; GUICHOT, "Acceso a la información…", cit., 2007, pp. 440-441; TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, pp. 98-99.
[2702] TRONCOSO REIGADA, "Transparencia administrativa…", cit., 2008, p. 68.
[2703] STJUE 9 de noviembre de 2010, Voljer und Markus Schecke GbR y otros v. Land Hessen, FJ 86.

Si la disociación desvirtúa por completo el ejercicio del derecho de acceso deberá plantearse la posibilidad de que se conozcan los datos asociados, incluso si afectan a la intimidad del titular. En estos casos la facultad de acceder a la información tomará en cuenta necesariamente determinadas medidas. Por un lado, el acceso deberá llevarse a cabo sólo a los datos estrictamente necesarios para satisfacer el interés de la persona que alega este derecho[2704]. Por otro lado, deberán adoptarse las medidas de seguridad que establece la Ley para fijar un control sobre el acceso que hayan podido realizar diferentes personas sobre las historias clínicas[2705]. Además, habría que considerar que el ejercicio de la ponderación no debería quedar en manos de los propios profesionales sanitarios frente a los que se ejerce el acceso, sino que debiera articularse un procedimiento concreto dirigido a realizar dicho juicio ponderativo. Como ha señalado la doctrina en alguna ocasión las agencias de protección de datos deberían jugar un papel fundamental en la resolución de estos conflictos[2706].

En conclusión, el derecho a la autodeterminación informativa no puede anular el derecho de acceso reconocido en la Constitución, pero el derecho de acceso, por el contrario, tampoco puede ejercerse de forma ilimitada sobre los ficheros que posee la Administración. Hay que atender a la importancia y las características de los intereses que colisionan en cada caso para encontrar el equilibrio entre ellos.

II. EL ACCESO A LOS DATOS POR CUENTA DE TERCEROS.

II.1. Introducción.

La actividad de la Administración, en general, y la de la Administración sanitaria, en particular, es cada vez más compleja y necesita de mecanismos que le permitan llevar a cabo sus funciones con la mayor agilidad y eficiencia posible[2707]. Pues bien, al igual que en el ámbito privado, la figura del outsourcing constituye en el ámbito de lo público un instrumento o actividad que se ha desarrollado, aunque en menor medida que en aquél[2708], para cubrir esa necesidad.

Ante las dificultades, sobre todo técnicas, que pueden surgir a la hora de llevar a cabo una actividad determinada, tanto las empresas privadas como las diferentes administraciones cuentan con la posibilidad de acudir a sujetos o entidades externas, preparadas y especializadas para realizar esas funciones, para que sean éstas las que gestionen ese servicio o lleven a cabo esa actividad concreta en su nombre[2709]. Este ejercicio de acudir a un sujeto externo es el que se conoce como outsourcing. Adelantando lo que se dirá en el apartado siguiente, esta figura

[2704] DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, pp. 544-546.
[2705] DEL CASTILLO VÁZQUEZ, *Protección de Datos…,* cit., 2007, p. 552.
[2706] GUICHOT, *Datos Personales…,* cit., 2005, pp. 347-348.
[2707] En el Código Tipo de la Unió Catalana D´Hospitals, artículo 11.1, se reconoce que "la complejidad cada día creciente de la asistencia sanitaria, socio-sanitaria y social, es un hecho incontestable que rara vez esta se puede llevar a cabo tan solo con los dispositivos y mecanismos de que dispone la entidad que realiza el tratamiento médico-sanitario del enfermo. El uso de servicios intermedios sanitarios externos (transporte sanitario, diagnóstico por la imagen, laboratorio, etc.) y la realización de técnicas diagnósticas y terapéuticas especializadas, entre otras, son elementos que justifican el acceso a los datos contenidos en los ficheros de pacientes".
[2708] DEL PESO NAVARRO, *Manual de Outsourcing…,* cit., 2003, p. 12.
[2709] FERNÁNDEZ SALMERÓN, *La Protección de los datos…,* cit., 2003, p. 252; SAÍZ PEÑA, "La Externalización…", cit., 2008, p. 276.

supone la externalización, desde una empresa privada o una Administración, de la realización de una determinada actividad de forma que ésta pasa a realizarse por un nuevo sujeto, que desarrollará esta función bajo la tutela del ente principal que contrata ese servicio y que mantiene la titularidad sobre el mismo[2710].

En el ámbito sanitario esta figura tiene recorrido, en lo que aquí interesa, en dos direcciones. A) En primer lugar, el outsourcing puede dirigirse a cubrir necesidades relacionadas, exclusivamente, con la manipulación de datos. El entramado institucional que compone la Administración sanitaria genera unas corrientes de información cuya gestión no es tarea fácil. La necesidad de que los datos fluyan sin problema, de tal forma que lleguen a los destinos requeridos en el menor tiempo posible y de una manera sencilla, y de que se garantice la confidencialidad de los mismos, teniendo que adoptar para ello medidas con un alto componente técnico, hace que resulte imprescindible contar con personal especialmente preparado y medios adecuados. En ocasiones, ese nivel de especialización se encontrará en empresas, órganos o personas que se sitúan fuera de la propia Administración que es responsable de la información[2711]. No es, por lo tanto, de extrañar que en el ámbito sanitario se acuda a sujetos externos, para que la gestión de la información de la que disponen los responsables de los ficheros sea la más eficiente posible, y la más respetuosa con los derechos fundamentales posible[2712]. En el ámbito de la CAPV, por ejemplo, el empleo de esta técnica está ya previsto por la disposición que crea los ficheros de Osakidetza[2713].

De esta manera, ha sido muy común en este sector la externalización de la labor de gestionar el tratamiento, la conservación y mantenimiento de las historias clínicas[2714]. Hay que tener en cuenta que estos documentos constituyen fuente constante de información para los diferentes profesionales que componen la Administración sanitaria. Ya se ha apuntado que son múltiples los accesos que se producen sobre ellas, generando así flujos constantes de datos. El control

[2710] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 179; DEL PESO NAVARRO, *Manual de Outsourcing*..., cit., 2003, p. 6, define el *outsourcing* como "la contratación por una organización de uno o varios proveedores externos para la prestación, mediante el empleo de activos ajenos a la estructura interna de aquella, de un servicio que anteriormente desarrollaba un departamento interno de la misma".

[2711] RUBÍ NAVARRETE, "Experiencia y Criterios…", cit., 2006, p. 272.

[2712] Resolución de la APDCM, "El contrato suscrito con una empresa privada para la implantación y gestión de la red informática en el área de sanidad no implica el acceso a datos clínicos de los pacientes a personas ajenas a la relación médico-paciente". Informe jurídico de la AEPD, "Informe de cumplimiento de la LOPD en Hospitales", octubre de 2010.

[2713] En el punto cuarto del Acuerdo de 19 de junio de 2006, del Consejo de Administración del Ente Público Osakidetza-Servicio Vasco de Salud por el que se regulan los Ficheros de Datos de Carácter Personal gestionados por Osakidetza-Servicio Vasco de Salud, se prevé que *"quienes, por cuenta de Osakidetza-Servicio Vasco de Salud, presten servicios de tratamiento de datos de carácter personal realizarán las funciones encomendadas conforme a las instrucciones del responsable del tratamiento y así se hará constar en el contrato que a tal fin se realice, no pudiendo aplicarlos o utilizarlos con fin distinto, ni comunicarlos ni siquiera para su conservación, a otras personas, de acuerdo con lo dispuesto en el artículo 12 de la mencionada Ley Orgánica 15/1999*".

[2714] Punto 3.b) Recomendación 2/2004, de 30 de julio, de la APDCM, sobre Custodia, Archivo y Seguridad de los Datos de Carácter Personal de las Historias Clínicas No Informatizadas: "en la actualidad se está extendiendo entre los centros sanitarios la práctica consistente en externalizar el tratamiento de las historias clínicas, a través de los llamados contratos de *outsourcing*. Por medio de los mismos, son entidades privadas, con personalidad jurídica distinta de la del responsable de las historias clínicas, quienes custodian los archivos". Recomendación de la AEPD "Plan de Inspección de Oficio sobre Tratamiento de Datos Personales en Laboratorios Hospitalarios", 2004. RUBÍ NAVARRETE, "Experiencia y Criterios…", cit., 2006, p. 276; DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 572.

estricto sobre este intercambio de información y la aplicación de las medidas de seguridad requeridas por la Ley sólo será posible si se cuenta con personal especializado y medios adecuados. En ocasiones, estos recursos se encontrarán fuera de la propia Administración sanitaria.

B) Desde una segunda perspectiva, el outsourcing puede darse cuando se externaliza otro servicio que no sea la labor de controlar la manipulación de la información sanitaria. Piénsese, por ejemplo, en la externalización de la labor de gestionar en nombre de una Administración sanitaria concreta material quirúrgico, principalmente, a efectos de que se lleve a cabo el pertinente control económico sobre el uso que se realice de dicho material[2715]. O el supuesto en que se externaliza la tarea de gestionar el servicio de llamadas de emergencia o de transporte sanitario[2716]. O los casos en que se contratan determinados servicios, como gestorías o asesorías jurídicas, para realizar funciones como el control de la contabilidad, o empresas determinadas para prestar servicios auxiliares, como podría ser el de asistencia psicológica[2717]. La gestión de cualquiera de estas tareas conlleva la manipulación de datos, por lo que si estas funciones se externalizan será necesario que quien vaya a llevarlas a cabo tenga acceso a la información.

En todas estas operaciones la entidad que se dedique a realizar la labor encomendada deberá tener acceso a los datos con los que cuenta la parte que la contrata, responsable de la citada información. Se producirá, por lo tanto, una transmisión de datos para que el sujeto externo pueda desarrollar su trabajo. Se puede decir, así lo hace la Ley, que este último accede a los datos por cuenta del responsable, pues lo hace para llevar a cabo la tarea encargada por dicho responsable, no para cumplir finalidades decididas por sí mismo. La relación que en este momento se crea entre quien transmite la información y la nueva entidad, que la recibe, plantea una serie de cuestiones que han de ser analizadas. Bien es cierto que en la práctica el outsourcing no ha sido una figura muy estudiada en referencia al tratamiento de los datos sanitarios. No obstante, esta circunstancia no quita para que se aclaren ciertos aspectos, que ayuden a tener una perspectiva general de lo que significa, de su contenido y de los problemas que plantea.

La regulación del acceso a los datos por parte del sujeto externo se ha realizado de manera bastante detallada en el ordenamiento, sin embargo, pueden encontrarse puntos polémicos que merecen ser comentados[2718]. La LPAC ya se acerca a esta figura al reconocer la posibilidad de que un órgano administrativo encomiende a otro órgano de la misma o de otra Administración la realización de determinadas tareas por razones de eficacia, sin que esta encomienda suponga la pérdida de la titularidad de la competencia o responsabilidad sobre dicha función[2719]. En relación

[2715] Informe jurídico de la AEPD 0406/2008.
[2716] Resolución de la APDCM, "Todo contrato suscrito por la Administración con un tercero para la prestación de un servicio que conlleve tratamiento de datos personales, queda sometido a la LOPD, especialmente a su artículo 12".
[2717] Código Tipo de la Agrupación Catalana de Recursos Asistenciales (ACRA), inscrito el 27 de diciembre de 2004.
[2718] DAVARA RODRÍGUEZ, *Guía Práctica de Protección…,* cit., 2006, p. 83.
[2719] Artículo 15 LPAC: "*1. la realización de actividades de carácter material, técnico o de servicios de la competencia de los órganos administrativos o de las Entidades de derecho público podrá ser encomendada a otros órganos o Entidades de la misma o de distinta Administración, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño. 2. la encomienda de gestión no supone cesión de titularidad de la competencia*

también a la actividad administrativa la nueva Ley de Contratos del Sector Público recoge, refiriéndose a la necesidad de respetar el derecho a la autodeterminación informativa cuando los contratos regulados en dicha Ley afecten a dicho derecho, una regulación que reproduce en gran parte lo dispuesto en la LOPD para el acceso a datos de carácter personal por cuenta de terceros[2720].

En el ámbito de la protección de datos, la LOPD, en cumplimiento de lo que ya disponía la Directiva europea[2721], abre la puerta a la figura del "acceso a los datos por cuenta de terceros" en su artículo 12, donde dice: *"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. 2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su*

ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda".

[2720] DA trigésima primera Ley 30/2007, 30 de octubre de 2007, de Contratos del Sector Público: "*1. Los contratos regulados en la presente Ley que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo.*

2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento.

En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán de constar por escrito.

Cuando finalice la prestación contractual los datos de carácter personal deberán ser destruidos o devueltos a la entidad contratante responsable, o al encargado de tratamiento que ésta hubiese designado.

El tercero encargado del tratamiento conservará debidamente bloqueados los datos en tanto pudieran derivarse responsabilidades de su relación con la entidad responsable del tratamiento.

3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:

a. Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.

b. Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.

c. Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.

En estos casos, el tercero tendrá también la consideración de encargado del tratamiento". FARRÉ TOUS, "El encargado del tratamiento…", cit., 2010, p. 1.108.

[2721] Artículo 16 Directiva 95/46/CE: "*Las personas que actúen bajo la autoridad del responsable o del encargado, incluido este último, sólo podrán tratar datos personales a los que tengan acceso, cuando se lo encargue el responsable del tratamiento o salvo en virtud de un imperativo legal*".

Artículo 17 Directiva 95/46/CE: "*1. Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales.*

Dichas medidas deberán garantizar, habida cuenta de los conocimientos técnicos existentes y del coste de su aplicación, un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse. (...)

3.La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular: -que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; -que las obligaciones del apartado 1, tal como las define la legislación del Estado miembro en el que esté establecido el encargado, incumben también a éste.

4. A efectos de conservación de la prueba, las partes del contrato y del acto jurídico relativas a la protección de datos y a los requisitos relativos a las medidas a que hace referencia el apartado 1 constarán por escrito o en otra forma equivalente".

celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar. 3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. 4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente". El reglamento que desarrolla la Ley entra a concretar distintos aspectos técnicos. Se recoge, por ejemplo, la posibilidad de que la labor a realizar por el encargado del tratamiento sea remunerada o no, indefinida o temporal. Se reconoce también la necesidad de que el responsable del fichero vele por el correcto cumplimiento del contrato firmado con el encargado[2722]. Se concreta, por otro lado, la posibilidad de subcontratar el servicio y las condiciones en que puede realizarse esta operación[2723]. Y por último determina la forma en que el encargado ha de conservar los datos a los que tiene acceso por motivo del cumplimiento de

[2722] Artículo 20 RDLOPD: "*1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.*
El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.
No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.
2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.
3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.
No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo".

[2723] Artículo 21 RDLOPD: "*1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.*
2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos: a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.
Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación. b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero. c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.
En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.
3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior".

sus funciones[2724]. En relación a la protección de los datos médicos, la Recomendación del Consejo de Europa simplemente señala que las personas que trabajen en representación de los profesionales sanitarios responsables de los ficheros estarán sometidas a las mismas normas de confidencialidad que pesan sobre dichos profesionales[2725]. Por su parte, la APDCat ha aprobado una recomendación dirigida a aclarar el régimen jurídico del encargado del tratamiento, que ha de tenerse en cuenta aunque sea a efectos interpretativos[2726]. De la regulación expuesta deberán deducirse los aspectos más relevantes de la figura que ahora se analiza.

II.2. Concepto.

Siguiendo lo que se ha dicho hasta ahora, el *outsourcing* vinculado al acceso a los datos por cuenta de terceros no sería más que el acto por el que el responsable de un fichero contrata o acuerda con un sujeto externo, que sea este último quien lleve a cabo una tarea que implica el tratamiento de unos datos, sin que por ello el responsable pierda la titularidad y la capacidad de decidir sobre qué hacer con los mismos.

En esta relación se distinguen dos sujetos, el que contrata o acuerda el servicio externalizado y el que va a realizar dicha tarea en nombre de aquél, que será el que materialmente manipule los datos. La LOPD define estas dos figuras. Denomina al primero "responsable del fichero o tratamiento" y lo define como la persona física o jurídica, pública o privada, u órgano de una Administración que determina qué datos se van a manipular, cómo y para qué[2727]. El segundo adquiere en la Ley el nombre de "encargado del tratamiento" y es definido como la persona, sea física o jurídica, pública o privada, que manipulará los datos en nombre del responsable[2728]. Estas definiciones se reproducen, prácticamente, en el reglamento que desarrolla la Ley[2729]. Las definiciones dadas por el Reglamento, sin embargo, han sido cuestionadas recientemente ante los tribunales. El principal punto de controversia lo constituía el que en la definición de "responsable del fichero o tratamiento" la disposición general señala que se mantiene esa

[2724] Artículo 22 RDLOPD: "*1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*
No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

[2725] Artículo 3.2 R (97) 5: "*Los datos médicos sólo pueden recogerse y procesarse si existen medidas de protección adecuadas establecidas por la ley nacional.*
En principio, los datos médicos deben ser recogidos y procesados sólo por profesionales sanitarios o por individuos u órganos que trabajen en representación de profesionales sanitarios. Los individuos u órganos que trabajen en representación de profesionales sanitarios recogiendo y procesando datos médicos deben estar sujetos a las mismas normas de confidencialidad que pesan sobre los profesionales sanitarios o las normas de confidencialidad comparables.
Los administradores de archivos que no son profesionales sanitarios sólo deben recoger y procesar datos médicos cuando estén sujetos a normas de confidencialidad comparables a las que pesan sobre el profesional sanitario o a medidas de seguridad igualmente eficaces proporcionadas por la ley nacional".

[2726] Recomendación 1/2010 APDCat, abril 2010, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña.

[2727] Artículo 3.d) LOPD.

[2728] Artículo 3.g) LOPD.

[2729] Artículos 5.1.i) y 5.1.q) RDLOPD.

condición, incluso, aunque no se realice el tratamiento materialmente. Esta cita no se recoge en la LOPD. Los tribunales han refrendado la validez de la definición dada por el reglamento al constatar que la situación recogida en la norma, en la que el responsable no llega a manipular los datos materialmente, puede darse cuando el tratamiento lo lleva a cabo un encargado, pero siendo el responsable quien marca las pautas a seguir en la manipulación[2730]. El responsable no pierde esta condición a pesar de que no manipule materialmente la información. Esta posición es la que aquí se analiza como acceso a los datos por cuenta de tercero.

En las normas quedan claras las funciones de cada sujeto: si bien es el encargado quien va a realizar o llevar a cabo las tareas encomendadas, el responsable seguirá manteniendo la titularidad de la competencia, y la capacidad de dirigir dicha labor y determinar los criterios que se habrán de seguir en su desarrollo[2731]. Es decir, en relación al tratamiento de datos, el encargado se erige en el sujeto que los manipula. Sin embargo, lo hace por cuenta del responsable del fichero, que es quien determina o define las finalidades de los tratamientos y la forma de llevarlos a cabo[2732]. El encargado no desarrolla finalidades propias sino que actúa para ejecutar los objetivos y las instrucciones del responsable. Como se ha dicho en alguna ocasión, parece que se establece entre ambos sujetos una relación jerárquica[2733]. En este sentido, si el encargado emplea la información a la que tiene acceso por cuenta del responsable para su propio beneficio, no se estará ante un acceso por cuenta de terceros sino ante una cesión de datos, a todos los efectos[2734].

La operación a la que se está haciendo referencia adquiere en la LOPD el nombre de "acceso a los datos por cuenta de un tercero". El empleo del término "tercero" en el enunciado del artículo 12 de la Ley genera cierta confusión. Parece que aquí el tercero hace referencia al responsable del fichero, pues el encargado accede a la información de carácter personal por cuenta del responsable. Sin embargo, lo lógico sería pensar que es el propio encargado el que debía ser considerado como "el tercero", persona ajena a la relación principal entre el titular de los datos y el responsable del fichero. En todo caso, si bien el enunciado pudiera llevar a equívocos, el contenido del artículo que se comenta no deja lugar a dudas sobre el papel de cada uno de los actores en esta operación[2735].

La importancia de definir la figura del acceso por cuenta de terceros viene dada por el riesgo de confundirla con la cesión de datos. Tanto cuando lo que se externaliza es la labor, exclusivamente, de manipular información, como cuando se trata de otra tarea que conlleva el tratamiento de datos, será necesario que se produzca entre el responsable y el encargado una

[2730] STS 15 de julio de 2010, FJ 4, se resuelve la legalidad de las definiciones dadas por el RDLOPD, que habían sido cuestionadas. Se subraya en dicha sentencia que en el reglamento, al igual que en la Ley, queda claro cuál es el papel de cada uno de los sujetos que participa en el tratamiento de unos datos.
[2731] GARCÍA DEL POYO VIZCAYA, "Encargado del tratamiento…", cit., 2010, p. 1.088.
[2732] STS 13 noviembre de 2007, FJ 2. CONDE ORTIZ, *La Protección de Datos…,* cit., 2005, p. 83; ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 201.
[2733] GOÑI SEIN, *La Videovigilancia Empresarial…,* cit., 2007, p. 144.
[2734] STS 9 de octubre de 2009, FJ 5. SAN 15 de octubre de 2004, FJ 5, en la que se sanciona a una asociación por haber empleado datos de salud de unos ciudadanos, cedidos por una fundación, para beneficio propio, concretamente para obtener donaciones de sangre por parte de los titulares de dichos datos. SAN 13 abril de 2005, FJ 4.
[2735] ULL PONT, *Derecho Público...*, cit., 2000, p. 131.

transmisión de datos. Evidentemente, sin dicha comunicación no será posible que el encargado realice sus tareas. En principio, esta operación constituye una revelación de datos equiparable a la que sucede en la cesión[2736]. Sin embargo, según apunta la LOPD no hay cesión de datos cuando el acceso a la información por parte del encargado se produce en nombre del responsable para el cumplimiento de las funciones encomendadas[2737]. Siempre y cuando se respeten los requisitos exigidos por la Ley y el reglamento que la desarrolla, la transmisión de datos no será considerada como una comunicación de datos y, lo que es más importante, no será necesario el consentimiento del titular de la información para llevarla a cabo. El principal efecto de considerar una operación como acceso por cuenta de tercero es la falta de necesidad de autorización de los titulares de los datos para llevar a cabo la transferencia de información. Teniendo en cuenta este efecto, el ordenamiento dispone que para poder interpretar una manipulación como acceso por cuenta de tercero se deberán cumplir todos los requisitos estipulados en el artículo 12. Este precepto constituye una unidad, sin que sus diferentes apartados puedan interpretarse como compartimentos estancos[2738]. Así, si alguna de las exigencias previstas por las normas no es respetada se entenderá que no se está ante un acceso por cuenta de tercero sino ante una cesión.

Más allá de su distinción con la cesión, el acceso por cuenta de terceros puede entenderse en un sentido amplio o desde una perspectiva más estricta. Desde esta segunda postura, se interpreta que entra en juego el artículo 12 de la LOPD cuando lo que se externaliza es, únicamente, la tarea de manipular los datos de carácter personal. Sólo se considerará que hay acceso por cuenta de terceros cuando lo que se encarga al tercero es exclusivamente el tratamiento de unos datos[2739]. No obstante, desde una perspectiva más amplia, se puede entender que existe *outsourcing* a efectos de aplicar la LOPD cuando lo que se externaliza es cualquier servicio que implique el tratamiento de datos de carácter personal[2740]. Como se ha podido intuir en el apartado anterior, se acoge aquí a la hora de interpretar el citado artículo 12 esta segunda postura. En diferentes informes jurídicos de la AEPD parece recogerse también esta posición, al reconocer la aplicabilidad de dicho precepto a supuestos en que lo que se externaliza no es exclusivamente la gestión de la información, sino servicios más generales[2741].

Esta perspectiva amplia ha podido generar problemas de interpretación, que han llevado a confundir, como ha ocurrido en la jurisprudencia, la figura del encargado del tratamiento con otras

[2736] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 219; RUBÍ NAVARRETE, "El Encargado del Tratamiento…", cit., 2008, p. 216.
[2737] Artículo 12.1 LOPD: "*No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento"*. Informes jurídicos de la AEPD 0350/2009 y 0411/2009.
[2738] STS 4 de mayo de 2009, FJ 2.
[2739] Es, por ejemplo, lo que parece deducirse de los informes jurídicos complementarios a la exposición realizada por el Consejero de Sanidad durante su comparecencia ante la comisión de Sanidad del Parlamento Vasco el 23/05/02 a fin de dar cuenta del proceso de centralización de los datos de los pacientes recogidos en los centros de Osakidetza, p. 22: "el artículo 12 de la LOPD regula aquellos supuestos en los que el responsable del tratamiento arrienda los servicios de un tercero para que realice el tratamiento de los datos personales por cuenta del responsable de los datos".
[2740] PICAZO SENTÍ y CHAVELI DONET, "El Tratamiento...", cit., 2002.
[2741] Informe jurídico de la AEPD 50/2006.

fórmulas jurídicas como puede ser el contrato de prestación de servicios[2742]. Los tribunales, en algún momento han llegado a decir que la regulación del artículo 12 de la Ley no se refiere a la figura del encargado del tratamiento sino que concierne a los requisitos que ha de cumplir el contrato de prestación de servicios por cuenta de terceros[2743]. Bien es cierto que la posición del encargado del tratamiento, independientemente de si ha sido contratado exclusivamente para manipular cierta información o para prestar un servicio más general, es semejante a la que nace del contrato de arrendamiento de servicios, pues en ambos casos un sujeto desarrolla una tarea para otro[2744]. En todo caso, independientemente de que la relación entre ambas personas sea calificada de una u otra forma, lo que hace el precepto objeto de análisis es determinar la situación de aquél que manipula datos de carácter personal en nombre de otro sujeto. Se entiende aquí que, a efectos de aplicación de la LOPD, incluso en el arrendamiento de servicios la prestación de servicios en nombre de quien los contrata puede constituir base suficiente para la aplicación del artículo 12 de la Ley, en cuanto que, si dicha tarea conlleva el tratamiento de datos, el sujeto contratado estará manipulando información en nombre de quien contrata dicho servicio. Esta manipulación de datos, si cumple con las condiciones exigidas por el ordenamiento, no será otra cosa que el acceso a datos por cuenta de tercero.

En un ámbito como el sanitario, donde la información vinculada a personas determinadas constituye un elemento fundamental en el funcionamiento diario de los centros, prácticamente todas las tareas que se llevan a cabo requieren de la manipulación de datos de carácter personal. La externalización de cualquiera de estos servicios conllevará una transmisión de datos. La aplicación de la perspectiva amplia comentada lleva a concluir que, independientemente de la fórmula jurídica que se emplee para contratar el servicio que sea, será necesario respetar lo dispuesto en el artículo 12 de la LOPD para que dicha transmisión de datos no sea considerada como una cesión.

A la hora de delimitar el ámbito de aplicación del concepto que se maneja, en algún caso se ha entendido, que para que se interprete que se está ante un acceso por cuenta de tercero será necesario que el encargado lleve a cabo la manipulación de datos a través de medios informáticos. Si no entrara en juego este tipo de herramienta se estaría ante una cesión y no ante un acceso por cuenta de terceros[2745]. Parece que la justificación de esta posición se basa en el hecho de que, en la práctica, la mayoría de los supuestos de externalización vienen motivados por las dificultades de la gestión informática de los datos de carácter personal[2746].

[2742] STS 29 de junio de 2010, FJ 2. En el ámbito de lo público este tipo de contrato se regula en artículo 10 Ley 30/2007, 30 de octubre de 2007, de Contratos del Sector Público: "*Son contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o un suministro. A efectos de aplicación de esta Ley, los contratos de servicios se dividen en las categorías enumeradas en el Anexo II*".

[2743] SAN 1 de febrero de 2006, FJ 3: que se refiere al artículo 12 LOPD como "precepto que no prevé la figura del "Encargado del tratamiento" (contrariamente a lo que erróneamente se aduce también en la demanda) sino que regula los requisitos que ha de reunir el contrato de prestación de servicios por cuenta de terceros, a efectos de excluir la cesión inconsentida de datos prevista en el artículo 11 de la repetida LOPD".

[2744] Artículo 1.544 CC: "*En el arrendamiento de obras o servicios, una de las partes se obliga a ejecutar una obra o a prestar a la otra un servicio por precio cierto*". APARICIO SALOM, *Estudios sobre la Ley*…, cit., 2000, p. 164.

[2745] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, pp. 164-166.

[2746] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 165.

Se entiende aquí que, si bien es cierto que en la gran mayoría de los casos el tratamiento de datos por parte del encargado se realizará empleando medios informáticos, no parece adecuado cerrar las puertas de la aplicación del artículo 12 de la LOPD a los supuestos en que esa manipulación se lleve a cabo manualmente[2747]. No se va a reproducir en este momento el debate en torno a la aplicabilidad de la Ley a los datos no automatizados[2748]. Hoy día está fuera de toda duda que también el tratamiento de los datos no informatizados está sujeto a la normativa de protección de datos[2749]. El hecho de que la LOPD sea aplicable a los ficheros manuales, parece que ha de ser argumento suficiente para comprender que todos los preceptos de la Ley se pueden alegar frente a todo tipo de ficheros, sean manuales o no.

II.3. Contenido.

II.3.1. Las garantías necesarias para que el acceso a los datos por cuenta de terceros no vulnere el derecho a la autodeterminación informativa.

El empleo del mecanismo de *outsourcing* puede considerarse positivo desde el punto de vista de la eficiencia. Supone trasladar una actividad concreta a un grupo de profesionales que exclusivamente se dedicarán a llevar a cabo el servicio contratado[2750]. La Administración o empresa responsable, en cierta medida, deja de preocuparse del ejercicio de una tarea cuya realización puede resultarle compleja[2751] y, sobre todo, el servicio externalizado pasa a llevarse a cabo de manera más eficiente por sujetos especialmente preparados para ello.

No es difícil reconocer en el ámbito sanitario las ventajas que puede plantear esta operación. Tanto para la gestión de la información contenida en las historias clínicas como para la prestación de otros servicios, la externalización puede constituir un instrumento que ayude a que la eficacia en el ejercicio de dichas tareas sea la máxima posible.

Sin embargo, más allá de las bondades de esta operación, pueden reconocerse también ciertos puntos oscuros. Cabe, por ejemplo, apuntar, el hecho de que un abuso del empleo, por parte de la Administración, del *outsourcing*, podría conllevar el peligro de dejar en manos de empresas privadas actividades que afectan al interés general[2752]. El principal peligro, sin embargo, se produce en relación al derecho a la autodeterminación informativa. Precisamente, de la afección de esta operación a dicho derecho nace la regulación que arriba se ha citado, que se dirige a proteger la facultad de todo ciudadano a controlar lo que sucede con sus datos cuando se da la externalización de un servicio.

[2747] MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 166: El propio autor entiende que el criterio que él plantea no hay que aplicarlo de forma estricta.
[2748] SAN 19 de mayo de 2004, FJ 2. PUENTE ESCOBAR, "Artículo 2…", cit., 2008, p. 51.
[2749] Artículo 2 LOPD. LESMES SERRANO, "Artículo 2…", cit., 2008, p. 69.
[2750] VILLAHERMOSA IGLESIAS, "Los Servicios...", cit., 2002, sugiere que "el dueño de un negocio no tiene porqué ser "experto en todo", y prefiere que otros que son profesionales en otros ámbitos, se encarguen, de manera más adecuada de una faceta de su empresa".
[2751] DEL PESO NAVARRO, *Manual de Outsourcing...*, cit., 2003, p. 26, apunta que la principal ventaja de esta institución "es el olvido (...) de la gestión informática y la posibilidad de dedicar todos los esfuerzos hacia otras áreas de la empresa".
[2752] TRONCOSO REIGADA, *Protección de Datos Personales…,* cit., 2008, p. 36.

El *outsourcing*, cuando implica un tratamiento de datos, conlleva necesariamente una nueva transmisión de información entre quien contrata el servicio y el contratista que va a realizar la labor encomendada. El sujeto contratado necesitará acceder a la información pertinente para poder realizar la tarea encargada. Esta transmisión, cabe recordar, no requerirá del consentimiento del titular de los datos. Como se dijera al analizar la cesión, toda transmisión, sobre todo si se realiza empleando herramientas informáticas, conlleva una multiplicación de los riesgos para el derecho a la autodeterminación informativa[2753]. Este riesgo se ha puesto de manifiesto en diversas ocasiones por parte de los tribunales. La posibilidad de que se transmitan los datos a un tercero, el encargado, sin necesidad de que se exija consentimiento del titular y, sobre todo, la posibilidad de que este tercero subcontrate a su vez esta tarea a otro sujeto, aumenta los riesgos de que los datos sean empleados de manera contraria a la Ley y de que el titular de los datos pierda el control sobre la información que le concierne[2754]. Evidentemente, cuanta más larga sea la cadena por la que pasan los datos, más lejano quedará para el titular el punto de referencia a la hora de controlar lo que sucede con los mismos y, sobre todo, a la hora de ejercer sus derechos[2755]. Será necesario, por lo tanto, sobre todo cuando se trata de datos que *a priori* requieren de una especial protección, que se adopten las garantías necesarias a la hora de llevar a cabo esta operación para proteger los derechos de los afectados. Una vez más hay que buscar el equilibrio entre la necesidad de externalizar ciertos servicios en aras de una mayor eficacia, y la protección del derecho a la autodeterminación informativa. Este equilibrio trata de buscarse en la normativa reguladora de la protección de datos.

En primer lugar, la LOPD no exige el consentimiento del titular para llevar a cabo la transmisión de datos que implica la externalización. La necesidad de adoptar todas las medidas posibles para proteger el derecho de cada uno a controlar lo que sucede con sus datos se ve reforzada, por lo tanto, por este hecho[2756]. La citada transmisión de la información es, sin duda alguna, una revelación de datos. Sin embargo, al considerarse que no se trata de una cesión de datos[2757], no es necesario el consentimiento del titular para ser llevada a cabo. Se entiende que la causa que motiva el principal tratamiento de los datos por el responsable (un negocio, una relación con la administración, el consentimiento del titular, etc.) motiva también la transmisión de los mismos en la externalización, sin necesidad de que se tenga que recabar el consentimiento del titular nuevamente. La justificación de esta situación reside en el hecho de que el encargado

[2753] SAN de 15 de noviembre de 2002, FJ. 4: "aunque jurídicamente no exista una cesión de datos, lo cierto es que materialmente la misma existe, lo que supone peligro o riesgo de publicidad del dato pues se encuentra en poder de un tercero distinto a aquel a quien afectado prestó su consentimiento". ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 204

[2754] SAN 21 de julio de 2004, FJ 4, en la que una empresa encarga a otra la realización de un servicio que conlleva un tratamiento de datos, y ésta última subcontrata, a su vez, otras dos empresas para realizar dicha tarea. Evidentemente, tal y como pone de manifiesto la decisión judicial, cuanto mayor es el flujo de información mayores riesgos hay de que se lleve a cabo un tratamiento de datos contrario a la Ley. ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 208.

[2755] BUISÁN GARCÍA, "Artículo 12…", cit., 2008, p. 314.

[2756] BUISÁN GARCÍA, "Artículo 12…", cit., 2008, p. 313.

[2757] Artículo 12.1 LOPD.

lo único que hace es manipular los datos por encargo del responsable, sin que tenga interés directo ni capacidad de decisión sobre ese tratamiento[2758].

La excepción a la exigencia de requerir el consentimiento puede hacer que parezca que en un inicio hay libertad absoluta a la hora de transmitir los datos al tercero encargado. Sin embargo, la Ley ha dispuesto una serie de medidas que hacen que esta operación se tenga que llevar a cabo con total seguridad y respeto a los derechos de los titulares de los datos.

En segundo lugar, habrá que atender a las garantías dispuestas por el ordenamiento para que la transmisión de la información sea respetuosa con dichos derechos. A) Como primera garantía, principios tan importantes como los que determinan la calidad de los datos permanecen plenamente vigentes[2759]. Por un lado, la transmisión sólo se llevará a cabo para cumplir la finalidad que motivó la recogida de datos por parte del responsable del fichero. Éste último no puede encomendar al encargado una tarea que implique emplear los datos de carácter personal para otros fines que no sean los que justificaron la recogida de dicha información. Por otro, el acceso por parte del encargado se realizará exclusivamente a los datos que sean estrictamente necesarios para que pueda llevar a cabo su labor. En cumplimiento del principio de proporcionalidad no es posible, por ejemplo, en la medida en que no es pertinente, que el responsable del fichero transmita datos estrictamente médicos al encargado del tratamiento, cuando éste está contratado exclusivamente para desarrollar labores de contabilidad[2760]. Por último, como es lógico, en la medida de lo posible los datos se transmitirán disociados. Sólo cuando sea necesario se revelarán los datos de forma que permitan la identificación de sus titulares[2761]. Como se ve, no hay una facultad ilimitada para transmitir esos datos.

B) Más allá de los principios citados, deberá respetarse también el derecho del titular a ser informado. El hecho de que la obligación de recabar el consentimiento se exceptúe no supone que con el derecho a ser informado ocurra lo mismo. El titular de los datos tiene pleno derecho a conocer cómo se manipulan los datos y quién accede a los mismos.

De una lectura literal de la Ley podría parecer que el derecho de información no tiene vigencia cuando se trata de externalizar los datos. Si esto fuera así, el titular de la información que se transmite al encargado no tendría conocimiento de lo que realmente sucede con los datos que le conciernen y quién los está manipulando efectivamente. El precepto que regula esta figura en la LOPD no dice nada al respecto. Tampoco lo hace el Reglamento que desarrolla la Ley. Ni

[2758] Informe jurídico de la AEPD 0363/2008, MESSÍA DE LA CERDA BALLESTEROS, *La Cesión...*, cit., 2003, p. 170, señala que no "se puede negar (...) que en estas prácticas existe revelación de datos de carácter personal, pero es obvio que el conocimiento de los mismos por parte del encargado no es el objeto directo del contrato, sino que su conocimiento es necesario para poder gestionar los ficheros".

[2759] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 224.

[2760] SAN 29 de marzo de 2006, FJ 8.

[2761] Punto 11.1 Circular 9/1997, de 9 de julio, del INSALUD, Instituciones generales sobre seguridad y protección de datos: "se deberán establecer compromisos de confidencialidad con aquellas empresas que traten datos del INSALUD, tales como empresas de servicios informáticos, laboratorios, empresas de almacenamiento de historias clínicas, u otras, asimismo se deberá exigir el cumplimiento por parte de éstas de medidas de seguridad de la información. Siempre que sea posible en los intercambios de información con estas empresas, se deberá evitar la identificación personal de los afectados. Los centros podrán reservarse el derecho de realizar controles periódicos para verificar el cumplimiento de dichas medidas".

siquiera a la hora de determinar el contenido de las notificaciones que se han de llevar a cabo para registrar tanto los ficheros públicos como privados se hace referencia alguna al encargado del tratamiento. El artículo 20 de la Ley, que determina el contenido mínimo que deberá recoger la disposición que creará, modificará o suprimirá los ficheros de titularidad pública, no hace mención a la figura del encargado del tratamiento. Tampoco lo hace el artículo 26, que concreta el contenido de la notificación de creación de los ficheros de titularidad privada, sin que estime obligatorio incluir referencia alguna sobre la externalización. No obstante, si se observan los formularios que la AEPD pone a disposición de los responsables de los ficheros para registrar sus ficheros, se verá que hay un apartado específico dedicado al encargado del tratamiento, en el que parece obligatorio declarar sobre la existencia de la externalización y la identidad del encargado[2762]. De la normativa expuesta no se puede deducir automáticamente que no se ha de informar sobre la existencia de la operación que ahora se analiza, cuando afecta a los datos de carácter personal de un sujeto.

Si bien se han podido plantear algunas dudas acerca de la vigencia del derecho a ser informado en la realización del *outsourcing*[2763], se entiende aquí que no hay motivo alguno para exceptuar dicho derecho en este caso. En la medida en que el derecho a ser informado, reconocido expresamente en el artículo 5 de la Ley, exige que el afectado conozca la existencia de todos los destinatarios a los que se dirijan los datos, no parece que se pueda excluir la externalización de esta obligación de informar. Necesariamente, el encargado del tratamiento, como tercero que tiene acceso a dichos datos, se erige en destinatario cuya existencia debe ser conocida. Hay que tener en cuenta además que el reglamento que desarrolla la LOPD reconoce la posibilidad de ejercer los derechos de acceso, cancelación, rectificación y oposición ante el encargado del tratamiento[2764]. Evidentemente, para que esta posibilidad sea ejecutable será necesario que el titular de los datos tenga conocimiento de la existencia, la identidad y dirección de dicho encargado. Siguiendo esta interpretación, en el ámbito sanitario se ha reconocido expresamente en algún protocolo de actuación la obligación de informar al titular de los datos sobre todos los destinatarios de la información, haciendo mención expresa a la necesidad de informar sobre los encargados del tratamiento[2765].

[2762] http://www.agpd.es/.

[2763] PICAZO SENTÍ y CHAVELI DONET, "El Tratamiento...", cit., 2002, entienden que es "aconsejable, que se informe a los interesados de la existencia de un tratamiento por terceros".

[2764] Artículo 26 RDLOPD: "*Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición*".

[2765] Artículo 6 Código Tipo de la Unió Catalana D´Hospitals, 22 de abril de 2004: "*Derecho de información en la recogida de datos. 1.- Los interesados a los que se recogen datos de salud, han de ser informados en ese momento de manera expresa, precisa e inequívoca de: c) los destinatarios de la información, que serán todos los departamentos en los que se organiza la entidad para poder llevar a cabo sus finalidades, así como las entidades públicas o privadas que por obligación legal o necesidad material, deban acceder a los datos a los efectos de la correcta prestación de la asistencia médico-sanitaria que constituye la finalidad del tratamiento de los datos".*
El artículo 11.2 del mismo código subraya la citada obligación cuando afirma que "*en estos casos no se está ante una cesión de datos, y por tanto no será necesario el consentimiento, si bien el documento de información referido en el artículo 6 de este Código Tipo deberán hacer mención genérica a esta transmisión de datos* (al *outsourcing*) *en el ámbito de las necesidades materiales de la correcta prestación del servicio".*

En lo que aquí interesa, teniendo en cuenta que será la Administración la que realizará el contrato de *outsourcing,* la obligación de informar se verá reforzada por principios que deben inspirar toda actuación del aparato público. Por un lado, el genérico principio de transparencia, que debe guiar toda relación entre las administraciones y los ciudadanos[2766], invita a que se haga una interpretación a favor del respeto del derecho a ser informado. Y por otro, el principio de publicidad que debe respetar todo contrato realizado por la Administración sugiere también que la operación de externalización sea conocida no sólo por el titular de los datos, sino también por toda la ciudadanía[2767].

C) Como principal garantía para la salvaguarda del derecho a la autodeterminación informativa la Ley prevé, para poder realizar un acceso a los datos por cuenta de terceros, la necesidad de formalizar un contrato entre el responsable del fichero y el encargado del tratamiento[2768]. Este contrato, más allá de la figura jurídica concreta que se quiera emplear para calificarlo[2769], podrá dirigirse exclusivamente a la fijación de las condiciones en que se tengan que tratar los datos, cuando el objeto del mismo sea precisamente el tratamiento de dichos datos, o podrá tener como objeto principal la prestación de otro servicio, si bien, en la medida en que dicha tarea conlleva necesariamente el tratamiento de datos de carácter personal, añadiendo una cláusula determinada referente a las condiciones que aseguren el respeto al derecho a la autodeterminación informativa. Podría pensarse que, al tratarse de un contrato, el principio de autonomía otorga plena libertad a las partes para disponer de los datos que van a ser objeto de transmisión. Sin embargo, como es lógico, dicho contrato se someterá plenamente a lo que establece la LOPD, sin que la voluntad de los contratantes pueda sobrepasar o contradecir las facultades y criterios que la norma establece para que el acceso por cuenta de terceros pueda realizarse[2770]. Este contrato se erige en el principal instrumento para controlar que la externalización se va a realizar de manera respetuosa con el derecho a la autodeterminación informativa. En este sentido, como bien ha subrayado la jurisprudencia, su finalidad es que quede

[2766] Artículo 3.5 LPAC: "*En sus relaciones con los ciudadanos las Administraciones públicas actúan de conformidad con los principios de transparencia y de participación".*

[2767] Artículo 1 Ley 30/2007, 30 de octubre de 2007, de Contratos del Sector Público: "*La presente Ley tiene por objeto regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los candidatos (...)*".

[2768] Artículo 12.2 LOPD: "*La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.*
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar".

[2769] GOÑI SEIN, *La Videovigilancia Empresarial…,* cit., 2007, p. 144.

[2770] SAN de 11 de febrero de 2004, FJ. 4, subraya que la "prestación de servicios regulado en este precepto (artículo 12) es una figura especial con regulación también especial, donde el objeto del contrato, tratamiento de datos de carácter personal, al afectar a las libertades públicas y a los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar, no puede quedar sometido dentro del tráfico mercantil al mismo régimen que las mercancías o prestaciones de servicios de contenido puramente patrimonial".
"Por tanto, la disponibilidad de las partes sobre el objeto del contrato no es tan fuerte como en otro tipo de relación contractual, sino que debe ceder a lo escrupulosamente determinado en la Ley, a fin de que tales derechos no puedan quedar afectados".

constancia de la forma en que se ha realizado, para poder controlar si la transmisión de datos se ha llevado a cabo de forma acorde a lo dispuesto por la Ley[2771].

II.3.2. La necesidad de que el contrato entre el responsable del fichero y el encargado del tratamiento cumpla con una serie de condiciones.

El contrato es un elemento constitutivo del acceso a los datos por cuenta de terceros. En caso de que el contrato no se formalice, o se realice sin tener en cuenta los criterios que marca la LOPD, y se lleve a cabo la transmisión se estará ante una cesión de datos común y no ante un acceso por cuenta de tercero[2772]. Si la justificación de la falta del consentimiento en los casos de externalización residía en la existencia de las garantías suficientes para poder llevar a cabo dicha transmisión de datos, cuando las garantías desaparecen desaparece también la posibilidad de calificar la operación como un mero "acceso a datos por cuenta de terceros".

El contrato se erige en el instrumento a través del que el responsable marca las pautas que el encargado deberá seguir en el tratamiento de datos. Si estas pautas son respetadas podrá decirse que el encargado accede a los datos por cuenta del responsable. En cambio, si no hay contrato que marque dichas pautas, o si el acuerdo no recoge todos los puntos que exige la Ley, se entenderá que el encargado no accede por cuenta del responsable, sino que lo hace por su cuenta. Así, el encargado se convertirá en un mero cesionario al que no se le han impuesto medidas específicas a seguir en el tratamiento de datos que vaya a llevar a cabo. Se estará ante una cesión, que necesitará para ser válida de los requisitos que establece la LOPD, es decir el consentimiento del titular de los datos o una causa justificativa recogida en la Ley[2773].

A) A la hora de formalizar el contrato no se especifica en principio la forma que éste deberá adoptar. Todo apunta, sin embargo, a que la forma escrita será la más adecuada, pues asegura su existencia[2774]. Ya de la anterior LORTAD podía deducirse, aunque de forma indirecta, la necesidad de que el contrato se fije de forma escrita. Recogía esta norma la expresión "*con fin distinto al que figure en el contrato de servicios*"[2775]. Como han señalado los tribunales, de esta redacción se intuía la necesidad de que el contrato se realizara de forma escrita, pues "figurar" hace referencia a la necesidad de que quede constancia de su existencia[2776]. En la norma hoy

[2771] STS 17 de abril de 2007.
[2772] Resolución de la AEPD, nº E/00523/2004, 18 de noviembre de 2005. BUISÁN GARCÍA, "Artículo 12…", cit., 2008, p. 314.
[2773] Como señala la AEPD en su resolución 00440/2004, de 27 de julio de 2004, "cuando no se cumplen las exigencias del citado artículo 12 no es aplicable el régimen jurídico que diseña la citada Ley para el encargado del tratamiento. Por tanto (...) ha de considerarse una cesión".
[2774] BUISÁN GARCÍA, "Artículo 12…", cit., 2008, p. 315; RUBÍ NAVARRETE, "El Encargado…", cit., 2008, p. 223.
[2775] Artículo 27.1 LORTAD.
[2776] SAN 15 de noviembre de 2002, FJ 4: "La regulación contenida en el artículo 27 de la Ley Orgánica 5/1992 no exige forma alguna en la celebración del contrato, por lo que en virtud del principio de libertad de forma –artículo 1.278 del Código Civil-, pudiera considerarse idónea la existencia de un contrato verbal (...), a diferencia de la regulación actual, por Ley Orgánica 15/1999 que limita la forma a que se haga "por escrito o en alguna otra forma que permita acreditar su celebración y contenido". Hay alguna sentencia que incluso ha llegado a argumentar que la propia LORTAD exigía de forma indirecta la forma escrita para la realización del contrato: SAN 15 de noviembre 2002, FJ 4: "La sala entiende que la intención del legislador al establecer en el artículo 27 de la LO 5/1992 era que existiese un contrato escrito por las siguientes razones:

vigente se exige expresamente la forma escrita o cualquier otra que permita acreditar su celebración y contenido[2777]. Podría llevar a confusión la referencia que se realiza en la Ley a la posibilidad de emplear "cualquier otra forma", pues podría interpretarse de tal modo que permitiese la forma verbal del contrato[2778]. Esta última opción sería aceptable en caso de que quedara constancia de la formalización del contrato, por ejemplo, a través de una grabación[2779]. Como la jurisprudencia ha aclarado, siendo la figura del acceso por cuenta de terceros una excepción al consentimiento en la cesión de datos, no cabe una interpretación amplia de la letra de la norma[2780]. En alguna resolución de la AEPD se ha llegado a afirmar que el contrato debe formalizarse de forma escrita[2781], sin embargo, en la mayoría de resoluciones reconoce la posibilidad de emplear otras fórmulas siempre y cuando permitan dejar constancia de su existencia[2782]. Es de subrayar que la nueva Ley de Contratos del Sector Público, que se refiere, en términos generales, a los diferentes tipos de contrato que puede formalizar la Administración, exige que, en caso de que la celebración de estos contratos conlleve un posible acceso a los datos por cuenta de terceros, los requisitos reconocidos en el artículo 12 de la LOPD se formalicen de forma escrita, sin admitir otra fórmula posible[2783]. Así lo hace también la recomendación de la APDCat. sobre la figura del encargado del tratamiento[2784].

1.- En primer lugar, porque así se infiere de una interpretación literal del artículo 27 de la LO 5/1992 al utilizar la expresión <<con fin distinto al que figure en el contrato de servicios>>, pues el término <<figure>> sólo tiene sentido en un contrato escrito.

2.- En segundo lugar, porque tal interpretación es la más acorde con la finalidad de la Ley. En efecto, la finalidad del art. 27 de la LO es regular el tratamiento de datos personales por terceros con base a un previo contrato de arrendamiento de servicios, no siendo preciso el consentimiento del interesado para esta <<cesión>> al existir una unidad jurídica entre el contratista y el responsable del fichero comitente. Ahora bien, aunque jurídicamente no exista una cesión de datos, lo cierto es que materialmente la misma existe, lo que supone peligro o riesgo de publicidad del dato pues se encuentra en poder de un tercero distinto a aquel a quien el afectado prestó su consentimiento. Por eso el legislador, exige al responsable del fichero diligencia en la elección del prestador del servicio y en la regulación del encargo, de modo que quede suficientemente garantizado que el prestador del servicio únicamente tratará los datos conforme a las instrucciones del responsable del fichero, que no los aplicará o utilizará con un fin distinto al pactado, y que no los comunicará ni conservará. Exigiendo la operatividad de esta finalidad, que el contrato sea escrito y en el queden nítidamente fijadas las condiciones indicadas. En otro caso, se generaría una situación de inseguridad jurídica en perjuicio del titular del dato.

3.- Que la finalidad del artículo 27 exige constancia escrita ser deriva del contenido del artículo 17.2 de la Directiva 95/46/CE (LCEur 1995/2977) donde se establece que la <<realización de tratamiento por encargo deberá estar regulada por un contrato o acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento>>, precepto que la doctrina interpreta en el sentido de que es preciso un contrato escrito. Y queda corroborada por el actual artículo 12 de al LO 15/1999 que habla expresamente de constancia por escrito".

[2777] Artículo 12.2 LOPD. STS 27 de marzo de 2007, FJ 3. En la que se subraya la necesidad de que la forma en que se celebre el contrato no sólo deje constancia de dicha celebración, sino también de su contenido.

[2778] RUBÍ NAVARRETE, "Experiencia y Criterios…", cit., 2006, p. 273.

[2779] SAN 3 de noviembre de 2004, FJ 3. STS 27 de marzo de 2007, FJ 3.

[2780] SAN 15 de noviembre de 2002 FJ 4: "Ciertamente el artículo 12 de la Ley también habla de <<constancia en alguna otra forma>> que permita acreditar la celebración del contrato. Pero estos términos no pueden interpretarse, como pretende el recurrente, en el sentido de que rige el principio de libertad de forma y es posible un pacto verbal, lo que sería contradictorio con que al mismo tiempo la norma exija la forma escrita. Lejos de ello lo que ocurre es que existen formas de formalización que pueden ofrecer garantías similares a la forma escrita (v. gr. Un supuesto de firma electrónica avanzada conforme a lo establecido en el Real Decreto-Ley 14/1999 [RCL 1999/2379], caso en el que no existiría un documento escrito en sentido estricto)".

[2781] Resolución de la AEPD nº E/00489/2008, de 1 de junio de 2009.

[2782] Resolución de la AEPD nº E/00007/2004, de 16 de mayo de 2005. Informe jurídico de la AEPD 0324/2009.

[2783] DA trigésimo primera Ley 30/2007, 30 de octubre de 2007, de Contratos del Sector Público: "*2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento.*

B) En cuanto al contenido, el contrato tiene que garantizar que el tercero conoce todos los aspectos que van a condicionar su trabajo en lo que concierne al tratamiento de los datos. En términos generales, deberá establecerse la finalidad a la que se destinará la manipulación. Se fijará la obligación del encargado de no comunicar la información de la que va a disponer. Se determinarán también los datos a los que el encargado va a tener acceso. Se concretarán otras instrucciones que el responsable tenga que dar al encargado. Por último, se fijarán las medidas de seguridad que el encargado deberá adoptar para garantizar la integridad de la información que manipulará[2785]. En la práctica, el cumplimiento de esta última exigencia necesitará de la puesta en común entre el responsable del fichero y el encargado del tratamiento, para que las medidas de seguridad sean efectivas, pues habrá que compatibilizar las medidas que cada uno deba adoptar. Al margen de lo establecido por la Ley la recomendación de la APDCat. va más allá y aconseja incluir unos contenidos complementarios a los citados, que aclaren con mayor exactitud el campo de actuación de este sujeto[2786].

Como se ha dicho, la falta de este contrato conlleva que la transmisión de datos que vaya a darse sea considerada, a efectos de aplicación de la Ley, como una cesión. Ya se ha argumentado que esta situación es comprensible. Sin embargo, cabe preguntarse si se dan las mismas consecuencias cuando existe contrato pero éste no contiene todos los elementos comentados. Las previsiones legales citadas parecen exigir que el contrato cuente con un contenido determinado, que es el arriba citado. Podría deducirse de ahí que si no respeta dicho contenido mínimo el contrato no será válido y que, por lo tanto, la transmisión no podrá considerarse un acceso a datos por cuenta de terceros. Esto podría llevar a pensar que por el mero hecho de que el contrato no haga referencia, por ejemplo, a las medidas de seguridad o al deber de secreto se entenderá que no es acorde a la Ley a la hora de configurar un acceso por cuenta de terceros. De esta manera la transmisión efectuada sería una cesión de datos realizada sin consentimiento, merecedora de la sanción correspondiente.

Respecto de esta cuestión no ha habido un pronunciamiento claro de los tribunales. Sin embargo, de sus decisiones podría deducirse la premisa de que cuando no concurren todos los contenidos previstos por la LOPD el contrato deja de tener validez y la transmisión pasa a convertirse en una cesión. En referencia al contrato verbal han señalado los tribunales que, para

En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 12.2 y 3 de la Ley Orgánica 15/1999, de 13 de diciembre. En todo caso, las previsiones del artículo 12.2 de dicha Ley deberán constar por escrito".

[2784] Capítulo 10.1 Recomendación APDCat 1/2010, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña

[2785] Artículo 12.2 LOPD.

[2786] Capítulo 1.7.2 Recomendación APDCat 1/2010, sobre el encargado del tratamiento en la prestación de servicios por cuenta de entidades del sector público de Cataluña: a) Identificación del fichero o ficheros que incluyen los datos; b) Posibilidad de que durante la ejecución del encargo se comuniquen los datos a otro encargado del tratamiento; c) Otras cesiones que, en su caso, haya autorizado el responsable del tratamiento; d) Si, al final de la prestación, el encargado tiene que devolver los datos y los soportes o documentos donde consten, los debe entregar a otro encargado que designó el responsable o las tiene que destruir. En caso de destrucción, se recomienda prever también que el encargado tenga que acreditarla ante el responsable mediante un certificado; e) Obligación del encargado del tratamiento de dar cumplimiento al deber de información, en caso de que recoja los datos; f) Determinación del procedimiento de atención del ejercicio de los derechos de acceso, rectificación, cancelación y oposición, para el caso de que la solicitud se presente ante el encargado del tratamiento; etc.

que se entienda válido a efectos de aplicar el artículo 12 de la Ley, será necesario demostrar que el mismo se ha celebrado y que tiene referencias expresas al contenido citado, a saber: instrucciones del responsable, la prohibición de que se van a emplear los datos para una finalidad distinta a la dispuesta y la prohibición de comunicar los datos por parte del encargado[2787]. En esta misma línea han apuntado los tribunales que la ausencia de las garantías previstas en el citado precepto de la Ley no constituyen meras irregularidades, sino que llevan a que la transmisión de datos tenga que calificarse como cesión[2788]. Bien es cierto que en esta afirmación se hace referencia a que han de cumplirse todas las garantías contenidas en el precepto y no que el contrato, concretamente, tenga que contener las cláusulas arriba citadas. Sin embargo, se entiende que la inclusión de dichas cláusulas en el contrato constituye en sí misma una garantía de entidad.

Podría pensarse que basta con que en el contrato quede constancia de que el encargado está actuando por cuenta del responsable, aceptando incluso cláusulas genéricas, para entender que se respeta el artículo 12. Sería suficiente una referencia general a que el encargado se somete a las instrucciones del responsable. Esto podría llevar a que cualquier contrato de arrendamiento de servicios, en la medida en que implica que el contratista queda sujeto a las instrucciones del contratante, sirviera para entender que se está ante un encargado del tratamiento a todos los efectos. Se entiende aquí que si se asumiera esta interpretación se estarían reduciendo las garantías mínimas para que el tratamiento de los datos por parte del encargado fuera respetuoso con el derecho a la autodeterminación informativa de los afectados. El responsable debe adoptar las medidas necesarias para que esa transmisión lleve a una manipulación de la información respetuosa con dicho derecho. Si no incorpora las cláusulas dispuestas por la Ley se entenderá que no recoge las garantías pertinentes, pues en ese caso el responsable no se estará asegurando de que el tratamiento que vaya a realizar el encargado sea

[2787] SAN 3 de noviembre de 2004, FJ 3: "el artículo 12.2 permite también el contrato verbal, siempre que se den dos condiciones:
1. Que pueda acreditarse la celebración del contrato.
2. Que se establezcan expresamente tres obligaciones del encargado del tratamiento (IC): a) únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento (el Ayuntamiento); b) no aplicará o utilizará los datos con fin distinto al previsto (la creación de un portal de Internet, con correo electrónico para los habitantes del municipio); c) no comunicará los datos, ni siquiera para su conservación, a otras personas". En el mismo sentido, pero referida a todo tipo de contratos, SAN 16 de febrero de 2005, FJ 3: "Para que concurra la figura del encargado del tratamiento el artículo 12.2 requiere, ya lo hemos señalado, que la relación entre el responsable del fichero y ese tercero al que se confiere el encargo quede regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido y que deberá incluir las especificaciones que el propio precepto legal determina". Esta decisión fue recurrida ante el TS, dictando éste STS 4 de mayo de 2009, FJ 2: "En primer lugar, el responsable del fichero debe haber encomendado el tratamiento de los datos mediante un contrato, pactado de forma que permita comprobar su existencia así como su contenido. En segundo término, dicha convención ha de contener las instrucciones que el responsable del tratamiento impone para el uso de los datos y de las que el encargado no puede separarse. Finalmente, tiene que constar también el fin que legitima la comunicación, que no pueden obviar las partes, quienes, además, han de abstenerse de comunicar los datos a otras personas".

[2788] SAN 11 de enero de 2006, FJ 5: "Como decíamos en una sentencia de esta Sala, de fecha 9 de febrero de 2002, (recurso 3-03) , esa ausencia de las garantías previstas en el artículo 12 no constituye un mero defecto o irregularidad en los términos alegados por la recurrente, sino que tiene el efecto esencial en este pleito de conllevar la aplicación del artículo 11 de la Ley 15/1999, cuyo apartado 1º establece con contundencia y claridad que el consentimiento previo del interesado también es imprescindible en los casos de comunicación de los datos de carácter personal objeto del tratamiento a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario..."; STS 14 de octubre de 2009, FJ 2.

acorde a las previsiones de la LOPD. El encargado, una vez tenga acceso a los datos, podrá actuar de acuerdo a la Ley o no, pero el responsable está obligado, en todo caso, a poner todos los medios posibles para que el tratamiento que vaya a realizar el encargado respete lo dispuesto en la Ley. Una de estas medidas será, sin duda alguna, la inclusión en el contrato a realizar con el encargado del contenido mínimo señalado.

II.3.3. Las obligaciones del responsable y el encargado en el acceso a los datos por cuenta de terceros.

A) Las obligaciones del responsable a la hora de formalizar el contrato son las siguientes. Es obligación del responsable que el contrato esté formulado de la forma antedicha. Deberá determinar claramente los parámetros que el encargado del tratamiento ha de respetar a la hora de manipular los datos, garantizando que el uso que se vaya a realizar de los mismos sea respetuoso con los derechos de las personas afectadas. En segundo lugar, estará obligado a notificar en el registro correspondiente los cambios que se produzcan con respecto a los ficheros que se vayan creando, modificando o suprimiendo fruto del tratamiento que el encargado realiza. Por último, según dispone el RDLOPD, el responsable estará obligado a "velar" porque el encargado cumpla con las condiciones que exige el ordenamiento[2789]. La doctrina ha puesto de manifiesto los problemas que plantea esta exigencia[2790]. Primero, habría que determinar qué condiciones debe garantizar el encargado, y segundo, cuál es el nivel de exigencia requerible al responsable a la hora de "velar" por el cumplimiento de dichas condiciones. A falta de pronunciamiento alguno por parte de la jurisprudencia sólo cabe interpretar la letra de la norma, tal y como ha hecho la doctrina.

Las condiciones se refieren a todas las obligaciones que el tercero ha de cumplir. En la práctica, sin embargo, no resulta fácil que el responsable pueda velar porque se cumplan determinadas condiciones, como por ejemplo, que el encargado emplee los datos para cumplir con la finalidad prevista o que no comunique los datos a otro sujeto. El encargado puede realizar esas acciones sin que el responsable tenga conocimiento de ello, por lo que velar por el cumplimiento de dichas obligaciones no resulta sencillo. Quizás, lo único por lo que efectivamente puede velar el responsable es porque el encargado adopte las medidas de seguridad necesarias para que la manipulación de los datos se realice en un entorno seguro. Se trata de medidas cuyo cumplimiento es controlable en la práctica. De la misma forma, la obligación de "velar" por el cumplimiento de dichas condiciones no puede llevar a exigir esfuerzos desproporcionados al responsable, a la hora de verificar que se cumplen las obligaciones pactadas. Debe bastar, se entiende aquí de acuerdo a la doctrina citada, con que el responsable se asegure de que el encargado se obliga a cumplir las instrucciones señaladas en el contrato, y realice controles periódicos de la actividad del encargado[2791]. En todo caso, parece difícil que en la práctica, ante un incumplimiento por parte del encargado, pueda demostrarse que existe responsabilidad del responsable del fichero. Podría darse esta circunstancia si, por ejemplo, se

[2789] Artículo 20.2 RDLOPD.
[2790] RUBÍ NAVARRETE, "El Encargado…", cit., 2008, p. 226; CHAVELI DONET, "El Estatuto del Encargado…", cit., 2009, p. 127.
[2791] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, pp. 226-228.

reconocieran indicios de que ante una infracción por parte del encargado el responsable tuviera conocimiento de la irregularidad y no hiciera nada para remediarla.

B) Por su parte, el encargado del tratamiento tiene que respetar los parámetros que le marca el contrato. Hay que tener en cuenta que este tercero no es más que un encargado, por lo que su margen de actividad es especialmente reducido, no pudiendo decidir por sí mismo el destino de los datos y teniendo que someterse a lo que dispone el contrato. De acuerdo con lo que establece la Ley[2792], el encargado estará sujeto también al deber de secreto, incluso cuando finalice su relación con el responsable del fichero[2793], y en este sentido, deberá asegurar que los empleados que componen la entidad cumplan con ese deber. El encargado no está obligado a inscribir el fichero en el registro correspondiente. En tanto que la inscripción ha sido llevada a cabo ya por el responsable del fichero, no es necesario inscribir por segunda vez el mismo fichero. Sin embargo, este sujeto sí estará obligado a informar al responsable sobre las modificaciones que se vayan sucediendo en los ficheros, con el fin de que este último pueda notificar esas circunstancias a la agencia correspondiente[2794]. Por último el encargado tendrá la obligación de tomar las medidas de seguridad necesarias para que el tratamiento de datos se realice en un entorno seguro. En este sentido, el RDLOPD determina expresamente medidas de seguridad que deberán adoptarse en el caso concreto de que exista un acceso a los datos por cuenta de terceros[2795].

En el momento en que el encargado lleve a cabo una actividad que no está prevista en el contrato, o que es contraria a lo dispuesto en el mismo, deja de ser considerado encargado del tratamiento para convertirse en responsable de fichero, lo que conlleva que deberá justificar el

[2792] Artículo 10 LOPD: "*Deber de secreto.- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del fichero".*

[2793] TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 105: "la empresa adjudicataria y el personal encargado de la realización de las tareas guardará secreto profesional sobre todas las informaciones, documentos y asuntos a los que tenga acceso o conocimiento durante la vigencia del contrato, estando obligado a no hacer públicos o enajenar cuantos datos conozcan como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo contractual".

[2794] DEL PESO NAVARRO, *Manual de Outsourcing...*, cit., 2003, p. 139.

[2795] Artículo 82 RDLOPD: "*1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.*

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento".

tratamiento de datos que haya realizado[2796]. Es lógica esta deducción por cuanto que, en la medida en que actúa de esta manera, el encargado no estará manipulando los datos por cuenta de nadie sino por cuenta propia. Así, será necesario que justifique ese tratamiento, generalmente, teniendo que contar con el consentimiento del titular. Es lo que ocurre, por ejemplo, cuando emplea los datos con una finalidad no prevista en el contrato o, como señala expresamente el reglamento, cuando el uso de la información se destina a la creación de una nueva relación entre el supuesto encargado y el afectado[2797]. En este último caso parece evidente que el encargado actúa por su cuenta, fuera de los parámetros establecidos por el contrato inicial[2798]. Cuando éste accede a los datos, no para prestar un servicio al responsable sino para realizar un uso de los mismos en beneficio propio, no podrá calificarse el acceso como un mero acceso por cuenta de terceros, por mucho que la transmisión esté autorizada por el responsable. En el momento en que el acceso se realiza para llevar a cabo una manipulación en beneficio propio, dicha transmisión deberá ser calificada como cesión[2799].

El régimen de sanciones que impone la LOPD no hace mención expresa al supuesto en que el encargado incumpla lo dispuesto en el contrato de *outsourcing.* No se recoge ninguna sanción específica para este tipo de infracción. No ocurre lo mismo en la legislación autonómica, donde se dispone, como consecuencia del incumplimiento del contrato por parte del encargado, además de las correspondientes sanciones, la resolución del contrato[2800].

La responsabilidad del encargado no sólo entra en juego cuando actúa de manera contraria a las instrucciones que se hayan podido determinar en el contrato. Es posible que esta responsabilidad surja también cuando el tratamiento de los datos se realiza siguiendo dichas indicaciones. La jurisprudencia ha puesto de manifiesto en diferentes ocasiones, que cuando el encargado vulnera lo dispuesto en la LOPD se convierte en responsable, incluso cuando ha actuado en nombre del responsable del fichero. En un supuesto en que un encargado comunicó a otra entidad los datos a los que tuvo acceso por cuenta del responsable, los tribunales sancionaron a dicho encargado por vulnerar la letra de la Ley, a pesar de que actuara siguiendo las instrucciones del responsable. Tiene plena coherencia esta interpretación por cuanto que a pesar de actuar en nombre del responsable el encargado también está sujeto a la letra de la Ley[2801].

[2796] Artículo 12.4 LOPD: "*En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente*". RUBÍ NAVARRETE, "Experiencia y Criterios…", cit., 2006, p. 273.

[2797] Artículo 20.1 RDLOPD: "*Se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado"*. SAN 20 de septiembre de 2003, FJ 2.

[2798] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, pp. 225-226.

[2799] STS 9 de octubre de 2009, FJ 4. SAN 13 de abril de 2005, FJ 4.

[2800] Artículo 9.4 Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid: "*el incumplimiento de las determinaciones indicadas en el apartado 2 del presente artículo será causa de resolución del contrato, sin perjuicio de las sanciones que eventualmente correspondan conforme a la Ley Orgánica 15/1999, de 13 de diciembre, y de las responsabilidades que pudieran derivarse por los daños y perjuicios que se ocasionen"*.

[2801] SAN 8 de octubre de 2003, FJ 5, en la que un club de football transmite una serie de datos a una empresa para que lleve a cabo en su nombre una finalidad incompatible con la que justificó la recogida de los datos. En este caso, sanciona el Tribunal al club de football por ceder la información sin consentimiento del titular y al encargado por

En este tipo de contratos la labor del encargado suele ser temporal. Según la Ley, cuando el servicio se acaba, y con él la necesidad de gestionar los datos, éstos deberán ser destruidos o devueltos al responsable junto a los soportes en los que se encuentran[2802]. Si el encargado del tratamiento empleaba soportes del responsable de los datos, éstos deberán ser devueltos al responsable una vez finalizado el encargo. Si, por el contrario, los soportes pertenecían al encargado, habrá de asegurarse de que una vez finalizado el servicio la información que contenían dichos soportes se borre. El reglamento, por su parte, desarrolla esta previsión[2803]. En primer lugar, realiza una matización sobre a quién debe el encargado devolver los soportes y los datos que ha empleado en la realización del servicio encomendado. En principio, se deberán devolver al responsable del fichero. Sin embargo, si éste último hubiera nombrado o contratado un nuevo encargado de tratamiento, el anterior encargado deberá devolver la información y los soportes a este nuevo encargado. Evidentemente, como bien ha señalado la doctrina, la transmisión de datos entre los diferentes encargados deberá realizarse con todas las garantías. Fundamentalmente, deberá quedar acreditada antes de la transmisión la condición de encargado del nuevo sujeto que va a tener acceso a los datos y deberá asegurarse que la transmisión se produce por orden del responsable[2804]. En segundo lugar, reconoce el reglamento la posibilidad de conservar los datos. Antes de aprobarse dicho reglamento, la AEPD había interpretado, partiendo de la LOPD, que como mucho podría admitirse la conservación de los datos por parte del encargado hasta que el responsable verificase si el cumplimiento del contrato ha sido correcto, habiendo establecido previamente un plazo máximo para llevar a cabo ese ejercicio de verificación[2805]. Parece que la previsión impuesta por el RDLOPD es más amplia que la interpretación realizada por la Agencia. Establece el reglamento la obligación de conservar los datos durante el tiempo que sea necesario, siempre y cuando dicha conservación esté justificada con el fin de esclarecer responsabilidades que pudieran derivar de la relación ente encargado y responsable[2806]. La conservación será posible también cuando una Ley lo prevea.

La LORTAD recogía una posibilidad distinta a la destrucción o borrado de los datos para cuando se fuera a resolver la relación entre el responsable y el encargado. Para los supuestos en que se previesen futuros contratos entre los mismos sujetos, se permitía que los datos permanecieran almacenados durante un período máximo de cinco años, siempre que mediara la autorización del responsable del fichero[2807]*.* Si bien desde el punto de vista de la eficiencia esta

manipular dichos datos sin consentimiento. SAN 21 de julio de 2004, FJ 4, en la que una empresa es sancionada por llevar a cabo una subcontratación contraria a la letra de la Ley, incluso habiéndolo hecho con conocimiento y consentimiento del responsable del fichero.

[2802] Artículo 12.3 LOPD.

[2803] Artículo 22 RDLOPD: "*1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*
No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.
2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento".

[2804] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 250.

[2805] Informe jurídico de la AEPD 283/2004.

[2806] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, pp. 252-253.

[2807] Artículo 27.2 LORTAD: *"Una vez cumplida la prestación contractual, los datos de carácter personal tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios,*

alternativa podría resultar positiva[2808], no ocurre lo mismo si lo que se valora es la falta de protección que esa medida puede conllevar de los datos objeto de tratamiento. En lo que aquí interesa, la posibilidad de que datos relativos a la salud puedan almacenarse durante 5 años por el mero hecho de que puedan ser necesarios en un futuro no se ve con buenos ojos. Se ha estado defendiendo en este trabajo la necesidad de que sólo en la medida en que sea necesario deberá manipularse la información sanitaria. Sin duda alguna, el que estos datos puedan conservarse durante el citado plazo con una finalidad no siempre clara aumenta innecesariamente los riesgos de que los datos se pierdan, se alteren o sean objeto de un acceso indeseado.

II.3.4. La subcontratación, una nueva figura reconocida en el RDLOPD.

El RDLOPD recoge una posibilidad que no se prevé en la LOPD. Es la facultad de subcontratar el servicio externalizado[2809]. De la letra de la Ley parecía desprenderse la imposibilidad de subcontratar por parte del encargado el servicio que realizaba en nombre del responsable del fichero. En la medida en que en la LOPD se prohíbe que el encargado transmita los datos a un sujeto que no sea el responsable[2810], no parece posible que la subcontratación se pueda dar, pues dicha operación conllevaría una transmisión de datos entre el primer encargado y el segundo[2811]. De inicio, el reglamento también prohíbe la posibilidad de subcontatación. Sin embargo, siguiendo las pautas marcadas anteriormente por informes jurídicos de la AEPD, posibilita después la realización de esta operación fijando diferentes opciones de

porque razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrán almacenar con las debidas condiciones de seguridad por un período de cinco años".

[2808] ULL PONT, *Derecho Público...,* 2000, p. 131, se pronuncia en el mismo sentido.

[2809] Artículo 21 RDLOPD: "*1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.*

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a. Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b. Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c. Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior".

[2810] ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 202.

[2811] SAN 21 de julio de 2004, FJ 4. PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 238; BUISÁN GARCÍA, "Artículo 12…", cit., 2008, p. 321.

subcontratar[2812]. En esta línea, también la ya citada Ley de Contratos del Sector Público reconoce la viabilidad de la subcontratación[2813].

Como expresa el reglamento, la subcontratación deberá realizarse por cuenta del responsable, con su autorización. Tiene sentido esta previsión, pues si la subcontratación se realizara sin dicha autorización se estaría ante una cesión de datos, pues la operación se estaría llevando a cabo a partir de decisiones independientemente tomadas por el encargado. Sin embargo, la subcontratación puede realizarse también sin autorización del responsable siempre y cuando se respeten ciertas garantías. Para que esto se produzca será necesario que en el contrato entre el responsable y el encargado del tratamiento se prevea la posibilidad de realizar dicha operación, concretando qué parte o tarea del servicio puede subcontratarse. Como bien ha señalado la doctrina, más allá de esta parte, será posible la subcontratación si se consigue la autorización del responsable[2814]. Será necesario también que se concrete la persona con la que se quiere subcontratar[2815], bien en el contrato o bien antes de realizar la subcontratación. Será obligatorio, además, que el tratamiento de datos por parte del subcontratista se ajuste a las instrucciones dadas por el responsable del fichero. Será necesario también que el encargado y el subcontratista formalicen un nuevo contrato distinto al celebrado entre responsable y encargado en los términos previstos por la LOPD y el Reglamento. Por último, si durante el tratamiento de datos por parte del encargado surgiera la necesidad de subcontratar un servicio y esta subcontratación no estuviera prevista en el contrato inicial, podrá subcontratarse dicho servicio siempre y cuando la subcontratación sea sometida al responsable en las condiciones anteriormente previstas. Esta previsión merece algún comentario. En primer lugar, para que esta operación pueda darse se requiere que la subcontratación sea necesaria. En caso contrario no será posible la realización de la transmisión. Evidentemente, se plantea un problema de interpretación a la hora de entender cuándo se considerará dicha operación como necesaria, pues confrontan criterios de eficiencia desde el punto de vista del mercado y criterios de seguridad jurídica desde el punto de vista de los titulares de los datos. En segundo lugar, se ha criticado el hecho de que este tipo de subcontratación sólo haya de ser "sometida al responsable". Se ha señalado que esta previsión podría abrir la puerta a una interpretación amplia de dicho concepto, en el que se otorgase cierta libertad al encargado para realizar la subcontratación. Se entiende aquí que el sometimiento al responsable se traduce en la necesidad de autorización del responsable[2816].

[2812] RUBÍ NAVARRETE, "El Encargado…", cit., 2008, pp. 232-233.
[2813] DA trigésimo primera Ley 30/2007, de 30 de octubre, Contratos del Sector Público: "*3. En el caso de que un tercero trate datos personales por cuenta del contratista, encargado del tratamiento, deberán de cumplirse los siguientes requisitos:*
a. Que dicho tratamiento se haya especificado en el contrato firmado por la entidad contratante y el contratista.
b. Que el tratamiento de datos de carácter personal se ajuste a las instrucciones del responsable del tratamiento.
c. Que el contratista encargado del tratamiento y el tercero formalicen el contrato en los términos previstos en el artículo 12.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
En estos casos, el tercero tendrá también la consideración de encargado del tratamiento".
[2814] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 241.
[2815] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, p. 242. Critica la inclusión de este concepto por cuanto que el encargado puede ser, más allá de una empresa, cualquier persona física, tal y como dice la propia LOPD.
[2816] PIÑAR MAÑAS, "Novedades en relación…", cit., 2008, pp. 244-245.

III. MOVIMIENTO INTERNACIONAL DE DATOS.

III.1. Introducción. La búsqueda de un equilibrio entre la necesidad de un flujo transfronterizo de datos y la protección del derecho a la autodeterminación informatiza.

Junto a la cesión de datos y el acceso a los datos por cuenta de terceros se reconoce en el ordenamiento otro supuesto de transmisión de información de carácter personal. Se está haciendo referencia a la operación que adquiere en la LOPD la denominación de "movimiento internacional de datos".

Hoy día es indiscutible que en prácticamente todos los ámbitos se producen manipulaciones de datos. La mayoría de las veces esos sectores cuentan con elementos o componentes de alcance internacional y cuando eso se produce, para que esos elementos puedan desarrollarse será necesario, entre otras cosas, que exista un flujo de información transfronterizo. En lo que toca a la seguridad, es conocido que la dimensión internacional que ha adquirido la lucha contra el terrorismo y otro tipo de delincuencia organizada lleva a que sea necesario un flujo constante de datos de carácter personal. Desde un punto de vista social, también es indudable que la circulación de las personas es cada vez mayor. La necesidad de controlar estos flujos obliga también a que sea necesaria la transmisión de datos entre diferentes países[2817]. En el sector económico, ya desde 1980 en el ámbito de la OCDE se reconocía expresamente la necesidad de que la protección de los datos de carácter personal no constituyera un obstáculo para el cumplimiento de fines económicos en sectores como la banca o los seguros[2818]. Esta misma previsión se recoge también en la Directiva europea de protección de datos, en la que se subraya la necesidad de que pueda darse un libre flujo de información en el ámbito europeo, y también en el internacional, que favorezca la realización de actividades económicas[2819]. Es conocido que el principal motivo que ha impulsado la realización de transferencias internacionales de datos y la necesidad de regular estas operaciones lo constituyen los intereses económicos[2820]. En el ámbito empresarial, la cada vez más habitual creación de grandes grupos de empresas multinacionales lleva a que se den transmisiones de datos que van más allá de las fronteras de un país determinado. Basta que una función determinada de dicha empresa multinacional, el departamento de recursos humanos, por ejemplo, esté centralizada en un punto concreto para que las transferencias sean constantes.

[2817] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 578.

[2818] Recomendación del Consejo de la OCDE relativa a las Directrices que rigen la protección de la intimidad y de la circulación transfronteriza de datos personales de 23 de septiembre de 1980, en la que se apuntaba que las "restricciones a esta circulación (de datos) podrían ocasionar graves trastornos en importantes sectores de la economía, tales como la banca y los seguros".

[2819] Considerando 7 Directiva 95/46/CE: "*Considerando que las diferencias entre los niveles de protección de los derechos y libertades de las personas y, en particular, de la intimidad, garantizados en los Estados miembros por lo que respecta al tratamiento de datos personales, pueden impedir la transmisión de dichos datos del territorio de un Estado miembro al de otro; que, por lo tanto, esta diferencias pueden constituir un obstáculo para el ejercicio de una serie de actividades económicas a escala comunitaria, falsear la competencia e impedir que las administraciones cumplan los contenidos que les incumben en virtud del Derecho comunitario; que estas diferencias en los niveles de protección se deben a la disparidad existente entre las disposiciones legales, reglamentarias y administrativas de los Estados miembros".* O el Considerando 56 Directiva 95/46/CE: "*Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional (...)*".

[2820] DEL PESO NAVARRO, "Las Leyes...", cit., 1997, "muchas veces nos olvidamos que el objetivo esencial de la Unión Europea es de tipo económico".

La necesidad de que en la práctica se produzcan transferencias internacionales de datos viene acompañada por el avance que las TIC han tenido en poco tiempo. Las nuevas tecnologías permiten que se superen las barreras espaciales y temporales que la realidad física impone y posibilitan, que el tratamiento de la información y en concreto su transmisión se realice de forma más rápida y a cualquier lugar del mundo. El flujo ilimitado de los datos de carácter personal ha encontrado en las TIC un aliado excepcional[2821]. En efecto, estas herramientas hacen que la manipulación de la información adquiera una dimensión global. Hoy día es normal, por ejemplo, que una información se recoja en un lugar, se almacene en otro y se manipule en un tercero distinto de los demás[2822]. Las transferencias internacionales son operaciones que cada vez se realizan más a menudo. Esta realidad se ve claramente reflejada en el aumento que en el Estado se ha producido de este tipo de transmisiones[2823].

Las transferencias internacionales generan riesgos evidentes para el derecho a la autodeterminación informativa. En primer lugar, el mero hecho de que se lleve a cabo una transmisión de datos crea peligros que han sido comentados durante este trabajo: el riesgo de que se pierdan, de que se alteren, de que sean aprehendidos por sujetos que quieran emplearlos de manera contraria a Derecho aumenta significativamente. En segundo lugar, el que la transmisión pueda realizarse a lugares donde las garantías de que el derecho a la autodeterminación informativa vaya a ser respetado sean menores a las dispuestas en el ordenamiento interno, conlleva un nuevo peligro que ha de ser considerado. Teniendo en cuenta que el nivel de protección que ofrecen los diferentes ordenamientos de los distintos estados es muy diferente y que incluso existen auténticos paraísos en los que dicha protección es prácticamente inexistente, es muy importante que se establezcan las garantías apropiadas para que estas transferencias puedan llevarse a cabo de tal forma que se asegure que los derechos y principios que componen el derecho fundamental a la autodeterminación informativa van a ser respetados[2824]. En tercer lugar, el hecho de que el flujo de datos tenga un alcance internacional implica, que aumentarán las probabilidades de que la capacidad de control por parte del titular de los datos de lo que ocurrirá con la información que le concierne se vea disminuida. El que el objeto de control se traslade fuera de las fronteras del Estado provoca que *a priori* resulte más complicado para los afectados asegurarse de que los parámetros que protegen su derecho a la autodeterminación informativa están siendo respetados. Por último, en cuarto lugar, la transferencia internacional provoca el riesgo de que, basándose en argumentos como la lucha contra el terrorismo, se generen grandes ficheros con una ingente cantidad de información sobre ciudadanos de múltiples estados.

Los particulares problemas que plantea el movimiento internacional de datos llevan a tener que analizar estas operaciones con cierta cautela. Se ha llegado a proponer incluso la conveniencia de que el Código penal recoja la transmisión de datos a los “paraísos informáticos” como un tipo agravado del delito de revelación de secretos[2825]. Resulta necesario encontrar el

[2821] ESTADELLA YUSTE, *La Protección…,* cit., 1995, p. 109.
[2822] ANCOS FRANCO, “La Regulación...”, cit., 1999, pp. 497-499.
[2823] Informe de la AEPD sobre Transferencias Internacionales de Datos, 2007, p. 5. La evolución del número de transferencias es significativa, pues pasa de las 2.614 de 2002 a las 8.483 de 2007.
[2824] CARRASCOSA LÓPEZ, “Circulación Internacional...”, cit., 1997, p. 510.
[2825] GÓMEZ NAVAJAS, *La Protección…,* cit., 2005, p. 317

equilibrio entre los distintos intereses en juego. Como se señalaba en el preámbulo del Convenio de 1981, es imprescindible la armonización entre la necesidad de que exista una libre circulación de información entre los pueblos y la necesidad de proteger la autodeterminación informativa de las personas[2826]. En la misma línea apuntaba la hoy derogada LORTAD, al subrayar la importancia de conciliar "*La protección de la integridad de la información personal (…) con el libre flujo de los datos, que constituye una auténtica necesidad de la vida actual de la que las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional pueden ser simples botones de muestra*"[2827].

La búsqueda de este equilibrio se ha visto reflejada en la práctica en diferentes ámbitos. Son numerosos los ejemplos que se pueden poner como exponentes del conflicto entre los intereses citados. Probablemente los supuestos más conocidos se refieren a las transferencias internacionales realizadas con el fin de combatir el terrorismo. Con este objetivo se han pretendido justificar operaciones cuya legalidad se ha puesto en duda en muchas ocasiones. Tras el atentado del 11-S se planteó, fundamentalmente por EEUU, la necesidad de controlar a los pasajeros que llegaran a dicho país. Para poder viajar a EEUU era necesario remitir determinada información a sus autoridades, lo que conllevaba la realización de una transferencia internacional de datos. El hecho de que en EEUU no exista un sistema de protección de datos equiparable al europeo llevó a que se planteara un serio y profundo debate en el seno de la UE sobre cómo se podían armonizar la necesidad de transmitir determinada información a EEUU, con el fin de garantizar la seguridad de dicho país, y la necesidad de proteger el derecho a la autodeterminación informativa de los pasajeros[2828]. A partir del 2002 el Grupo de Trabajo del artículo 29 de la Directiva emitió diferentes informes en relación a esta cuestión poniendo el acento en la necesidad de cohonestar el derecho a la autodeterminación informativa y la seguridad[2829]. Hoy día, tras la intervención incluso del TJUE[2830], la regulación de esta materia se realiza a través de un acuerdo firmado entre la UE y los EEUU[2831]. Se trata de un documento que ha generado numerosas dudas. Aunque en principio no se recoja la posibilidad de remitir información sensible, no queda claro que en un momento dado o en determinadas circunstancias

[2826] Preámbulo Convenio 108/1981 del Consejo de Europa. DEL PESO NAVARRO, *Ley de Protección…,* cit., 2000, p. 85.
[2827] Exposición de Motivos LORTAD.
[2828] La AEPD se opuso a la posibilidad de que se remitieran los datos de carácter personal a la aduana norteamericana sin el consentimiento expreso de los afectados, Datospersonales.org Revista de la APDCM, nº 2, 1 de mayo de 2003.
[2829] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos, 24 de octubre de 2002. Pueden consultarse las preguntas más frecuentes sobre la recepción por el Servicio de aduanas y protección de fronteras del registro de nombres de los pasajeros en relación con los vuelos entre la Unión Europea y Estados Unidos, en el Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 8/2004, de 30 de septiembre de 2004, sobre la Información a los Pasajeros relativa a la Transferencia de Datos PNR (*Passenger Name Records*) sobre los Vuelos entre la UE y los EEUU de América.
[2830] STJUE, 30 de mayo de 2006, Parlamento Europeo v. Consejo de la Unión Europea.
[2831] *Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carries to the United States Department of Homeland Security (DHS)*, 23 de julio de 2007. DO nº L-204/18, 4 de agosto de 2008. Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2007, relativo a la información de los pasajeros en relación con la transferencia de datos PNR a las autoridades de los Estados Unidos, 15 de febrero de 2007 y actualizado el 24 de junio de 2008.

no pueda realizarse[2832]. En relación a la posibilidad de remitir información sobre los pasajeros que se dirigen a los EEUU, se planteó también la posibilidad de que se remitieran datos de salud con el fin, esta vez, de prevenir epidemias. Esta posición fue valorada muy negativamente por el Grupo de Trabajo del artículo 29, por atentar contra los principios que fundamentan la Directiva[2833].

La lucha contra el terrorismo se ha convertido también como argumento principal para tratar de justificar otro tipo de transferencias. Se está hablando fundamentalmente de los movimientos que se puedan generar en el ámbito de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (SWIFT). Como ya puso de manifiesto el Grupo de Trabajo del artículo 29, esta entidad realiza una labor de mensajería financiera mundial que facilita transferencias internacionales de dinero. Esta sociedad almacena todos estos mensajes durante un determinado período de tiempo y los conserva físicamente en dos centros: uno en la UE y otro en EEUU. Con el objetivo de luchar contra el terrorismo las autoridades estadounidenses requirieron que se facilitara el acceso a dicha información[2834]. El Parlamento Europeo, tras rechazar previamente esta posibilidad por entender que se trata de una actividad que no respeta las garantías mínimas de protección de datos[2835], ha aceptado finalmente el acuerdo que permite la transmisión masiva de datos[2836]. La polémica generada en torno a esta previsión ha llevado al citado grupo de trabajo a mostrar su desacuerdo con este convenio, debido a las escasas garantías que presenta con respecto a la protección del derecho a la autodeterminación informativa[2837].

El conflicto entre la necesidad de transmitir información de carácter personal a otros estados y la obligación de proteger el derecho a la autodeterminación informativa ha tenido también eco en el sector de la sanidad. En este ámbito la transferencia internacional de datos no es una operación muy común, si se compara con otras áreas de actividad como puede ser la de telecomunicaciones o la empresarial[2838]. No obstante, como en alguna ocasión han puesto de manifiesto las memorias de la AEPD, este tipo de transmisión ha afectado también a los datos sanitarios. Concretamente, la memoria de 2004 apunta que se notificaron durante ese año 57

[2832] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 5/2007 relativo al nuevo Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros (PNR) por parte de las compañías aéreas al Departamento de Seguridad del Territorio Nacional de los Estados Unidos, 17 de agosto de 2007.

[2833] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2006 sobre la notificación de la propuesta de Reglamento del "US Deparment of Health and Human Services", de 20 de noviembre, relativo al control de las enfermedades contagiosas y a la obtención de información sobre los pasajeros, 14 de junio de 2006.

[2834] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 10/2006, sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*- SWIFT), 22 de noviembre de 2006.

[2835] "El Parlamento Europeo rechaza formalmente la transferencia de datos bancarios a EEUU"*, El País*, 11 de febrero de 2010.

[2836] "La UE y EEUU firman el acuerdo para intercambiarse datos bancarios"*, El País*, 28 de junio de 2010.

[2837] Decisión del Consejo Europeo, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo, 24 de junio de 2010.

[2838] Informe de la AEPD sobre Transferencias Internacionales de Datos, 2007, 7. El 58 % de las transferencias realizadas responden a finalidades relacionadas con la gestión empresarial.

tratamientos con transferencias internacionales que afectaban a este tipo de información[2839]. Posteriores memorias no han entrado a detallar este dato, sin embargo, es de suponer que estas operaciones han ido aumentando en la práctica, en la medida en que cada vez son más los instrumentos y proyectos que en el ámbito sanitario tienen alcance internacional[2840] y que incluso las propias normas crean situaciones que reclaman este tipo de transferencias[2841]. La transmisión de datos de salud más allá de las fronteras estatales puede responder a motivos sanitarios o para cumplir otras finalidades como la emisión de contratos de seguros o la correcta tramitación de los siniestros[2842].

El hecho de que las transferencias internacionales también tengan cabida en el ámbito sanitario debería encontrar reflejo en los diferentes registros de las distintas agencias de protección de datos. En principio, dispone la LOPD, cuando se pretende realizar una transferencia de alcance transfronterizo, esta circunstancia debe constar en los documentos que crean o modifican los distintos ficheros que contienen los datos de carácter personal, sean públicos o privados[2843]. Estos ficheros deberán ser inscritos en los diferentes registros. Por lo tanto, debería poder encontrarse alguna referencia a las transferencias internacionales de los datos sanitarios en dicho órgano. Es paradójico, en este sentido, que, salvo casos excepcionales, como el recogido en relación del Registro Nacional de Sida[2844], en el ámbito sanitario no se encuentren anotaciones referentes a las posibles transferencias internacionales que de estos datos puedan realizarse.

Sea cual sea el caso, parece clara la preocupación que estas operaciones generan desde el punto de vista de la protección de datos. La necesidad de crear un entorno global seguro en el que se puedan llevar a cabo las transferencias internacionales con la garantía de que se va a respetar el derecho a la autodeterminación informativa en todos sus componentes se ha puesto de manifiesto en reiteradas ocasiones. Recientemente las autoridades de protección de datos y privacidad de diferentes países han tratado de definir unos criterios comunes que aseguren, entre

[2839] Memoria de la AEPD 2004. En 2002 fueron 27 las operaciones de este tipo que se realizaron, según Memoria de la AEPD 2002.

[2840] TRONCOSO REIGADA, *Guía de protección…,* cit., 2004, pp. 49-50.

[2841] Artículo 6 RD 2210/1995, 28 de diciembre de 1995, por el que se crea la Red Nacional de Vigilancia Epidemiológica: "*El Ministerio de Salud y Consumo: (...)*
2. Coordinará las acciones e intercambios de la información correspondiente a la vigilancia epidemiológica tanto a nivel nacional como a nivel de la Unión Europea, Organización Mundial de la Salud y demás organismos internacionales.
3. Propiciará el cumplimiento de las obligaciones sanitarias internacionales, como son la notificación internacional de las enfermedades cuarentenables y la de aquellas que son objeto de vigilancia especial por la Organización Mundial de la Salud y la Unión Europea".

[2842] Resolución de la AEPD, Expediente nº TI/00017/2009, de 11 de mayo de 2009.

[2843] Artículo 20.2 LOPD: "*Las disposiciones de creación o de modificación de ficheros* (de las Administraciones públicas) *deberán indicar: (...)*
e. Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros".
Artículo 26.2 LOPD: (en relación a los ficheros privados) "*Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros*".

[2844] http://www.agpd.es

otras cosas, unos estándares internacionales de protección de datos que hagan que las transferencias se realicen de forma más segura[2845]. En este sentido el ordenamiento trata de regular esta figura, de tal manera que los movimientos internacionales de datos se realicen de forma que el derecho a la autodeterminación informativa se vea afectado en la menor medida posible.

III.2. Definición del concepto "transferencia internacional de datos" y referencia a su regulación en la normativa de protección de datos.

No se realizará en este capítulo un análisis detallado de todos los aspectos que rodean a la transferencia internacional de datos, sino que se intentarán exponer las principales garantías que estas operaciones han de cumplir para ser respetuosas con el derecho a la protección de datos. Para ello habrá de fijarse principalmente en el texto de la LOPD, que pese su amplitud aquí se reproduce. Establece la Ley en el artículo 33 que *"1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia Española de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.*

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia Española de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". Sin embargo, establece después en el artículo 34 una serie de excepciones a esta regla, entre las que se incluye expresamente la posibilidad de transmitir datos de salud a países que no presten un nivel equiparable de protección por motivos sanitarios: "Lo dispuesto en el artículo anterior no será de aplicación:

a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España;

b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional;

c. Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios;

[2845] *Propuesta conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de Carácter Personal,* acogida por la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Madrid, 5 de noviembre de 2009.

d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica;

e. Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista;

f. Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado;

g. Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero;

h. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias;

i. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

j. Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo;

k. Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado".

La letra de la Ley es fruto de la transposición de la Directiva 95/46/CE[2846] y es desarrollada en el RDLOPD[2847], que incorpora, en gran parte, la Instrucción 1/2000 de la AEPD, de 1 de diciembre, relativa a las Normas por las que se rigen los Movimientos Internacionales de Datos[2848]. Esta Instrucción no ha sido derogada expresamente por el nuevo Reglamento de desarrollo de la LOPD, si bien en lo que contradiga al Reglamento no tendrá aplicación. Lo cierto es que en la práctica la Instrucción no se emplea hoy día como fundamento para otorgar autorizaciones de transferencias internacionales o resolver otras cuestiones que atañen a este tipo de operaciones por la AEPD. El contenido de la Instrucción generó cierta polémica y fue anulado en algunos apartados por los tribunales, por otorgar a la AEPD mayores facultades de las que en un inicio le asigna la LOPD en el ejercicio de control de las transferencias internacionales que no requieren de la autorización del Director de la Agencia[2849]. En todo caso la Instrucción deberá tenerse en cuenta para analizar el régimen jurídico vigente que regula la transferencia internacional de datos. Más allá de estos textos normativos, habrá que atender a la hora de interpretar la Ley a la Recomendación (97) 5, a las diferentes decisiones que la Comisión Europea ha adoptado al respecto, y a las aclaraciones realizadas por el Grupo de Trabajo del artículo 29 de la Directiva.

[2846] Artículos 25 y 26 Directiva 95/46/CE.
[2847] Artículos 65 a 70 RDLOPD.
[2848] BOE nº 301, 16 de diciembre del 2000.
[2849] SAN 15 de marzo de 2002 y STS 25 de septiembre de 2006.

Conviene, en primer lugar, fijar una definición de lo que se entiende por transferencia internacional de datos de carácter personal. Ni la LOPD ni la Directiva europea aclaran este extremo. Antes de la entrada en vigor del RDLOPD, la Instrucción de la AEPD que regulaba los movimientos internacionales de datos disponía que "*se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español*"[2850]. Según el reglamento actualmente derogado, que, siguiendo la básica definición que anteriormente se había aportado desde la OCDE[2851] y el Consejo de Europa[2852], desarrollaba la LORTAD, el citado concepto ha de entenderse como "*el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional*"[2853]. Hoy día, esta definición ha sido matizada en el reglamento vigente que desarrolla la LOPD, que define la transferencia internacional de datos como el "*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español*"[2854]. Por su parte, define al "exportador de datos personales" como "*la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero*" [2855] y al "importador de datos personales" como "*la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero*"[2856].

La definición que se ha dado en el RDLOPD de transferencia internacional de datos merece alguna aclaración. A) En primer lugar, cabe criticar la exclusión que se hace en dicha definición de las transmisiones que se vayan a realizar en el Espacio Económico Europeo. Tanto la Directiva[2857] como el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[2858], señalan que no se pueden restringir los flujos entre los estados miembros. El Reglamento da un paso más y deja de considerar estas operaciones como transferencias internacionales[2859]. La LOPD, por su parte, hace una consideración diferente sobre este tipo de operaciones. Entiende que las transmisiones

[2850] Norma primera Instrucción de la AEPD 1/2000, de 1 de diciembre del 2000, relativa a las Normas por las que se rigen los Movimientos Internacionales de Datos.
[2851] Directriz 1.c) Recomendación OCDE, sobre directrices que regulan la protección de la privacidad y el flujo internacional de datos de carácter personal, 1980: "*transborder flows of personal data" means movements of personal data across national borders*".
[2852] Artículo 12 Convenio 108/1981 del Consejo de Europa.
[2853] Artículo 1.6 RD 1332/1994, 20 de junio de 2004, por el que se Desarrollan Algunos Puntos de la LORTAD.
[2854] Artículo 5.1.s) RDLOPD.
[2855] Artículo 5.1.j) RDLOPD.
[2856] Artículo 5.1.ñ) RDLOPD.
[2857] Artículo 1.2 Directiva 95/46/CE: "*Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1*".
[2858] Artículo 12.2 Convenio 108/1981 del Consejo de Europa: "*Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte"*.
[2859] FATÁS y GARCÍA SANZ, "Título Primero…", cit., 2008, p. 140.

realizadas dentro de la UE tienen la consideración de movimientos internacionales, si bien se trata de operaciones privilegiadas que quedan excluidas del régimen jurídico general que regula estas operaciones[2860], de tal manera que las transmisiones dentro de este espacio pueden llevarse a cabo con mayor libertad[2861]. Al existir en los países que configuran la Unión un sistema de protección equiparable al establecido en el ordenamiento interno, las transmisiones se realizan como si de una cesión se tratara, sin necesidad de controles específicos del Director de la AEPD[2862]. Si bien tanto en el caso de la Ley como en el del Reglamento que la desarrolla se trata de otorgar libertad a los movimientos realizados en este entorno, se entiende aquí que el punto de partida ha de ser la consideración de toda transmisión a un país extranjero como una transferencia internacional. Hay que resaltar que algún informe jurídico de la Agencia, antes de la aprobación del actual reglamento que desarrolla la Ley, ha tratado las transmisiones dentro de la UE como transferencias internacionales[2863]. Si bien debería referirse al Espacio Económico Europeo, por aplicarse la Directiva también en los países de dicho ámbito que no pertenecen a la UE, la previsión de la Ley se entiende, al contrario de lo que se ha subrayado por parte de la doctrina[2864], más afortunada. Al incluir estos movimientos en la disposición que regula las excepciones al régimen general, la Ley interpreta que se trata de operaciones que debido a las circunstancias en que se producen han de ser objeto de una regulación privilegiada, al igual que los demás casos recogidos en el artículo 34. Si bien desde el punto de vista práctico puede que las consecuencias de esta consideración no sean especialmente relevantes, desde una perspectiva conceptual no cabe duda que tiene su importancia. Esta relevancia se revela sobre todo a la hora de inscribir la operación en el registro. En beneficio de una mayor claridad se considera aquí positivo que incluso este tipo de tratamientos se notifiquen a la Agencia como transferencias internacionales.

B) En segundo lugar, la referencia que en la definición se realiza a la cesión y al acceso a los datos por cuenta de terceros podría causar problemas de interpretación, pues podría llevar a entender el concepto de transferencia en un sentido especialmente amplio. Se podría considerar que estos movimientos con alcance supranacional no son más que cesiones o accesos internacionales. Así se ha hecho en algún caso por parte de la doctrina, sin bien para justificar la aplicación de las garantías referidas a la cesión a los supuestos de transferencia internacional[2865]. A ello podría llevar también la definición que la Instrucción de la AEPD daba de esta operación, al referirse a ella como "*toda transmisión*" de datos. De esta consideración podría deducirse que la publicación de una información, por ejemplo, en Internet constituye una transferencia internacional de datos. Teniendo en cuenta el alcance de esta herramienta informática esta conclusión sería perfectamente posible, pues unos datos hechos públicos en este medio serían accesibles desde cualquier rincón del planeta, tanto desde los que presentan

[2860] Artículo 34.k) LOPD.
[2861] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 579.
[2862] STS 25 de septiembre de 2006, FJ 4. Informe de la AEPD sobre Transferencias Internacionales de Datos, 2007, p. 29.
[2863] Informe jurídico de la AEPD 0493/2005, en la que se trata una transferencia al Reino Unido como movimiento internacional de datos.
[2864] SANCHO VILLA, *Negocios Internacionales*..., cit., 2010, pp. 23-24, considera felicita la regulación realizada por el RDLOPD.
[2865] COUDERT, "Transferencias Internacionales…", cit., 2007, p. 429.

un nivel de protección de datos equiparable al español y como desde los que no presentan ninguna protección.

No parece que el legislador esté pensando en este supuesto cuando regula la transferencia internacional. Así lo ha subrayado el TJUE en una conocida y esclarecedora decisión[2866]. Se señala en la misma que si se comprendiera que la publicación en Internet conlleva una transferencia internacional de datos, lo más probable es que la mayoría de dichas publicaciones no podrían llevarse a cabo, por cuanto que en todo caso se tendría acceso a los datos publicados desde países terceros que no garantizan una protección equiparable a la establecida en el ordenamiento interno[2867]. Como luego se verá, es necesario cumplir con unos requisitos especialmente estrictos para que las trasmisiones a este tipo de países puedan llevarse a cabo. Si la publicación en Internet constituyera una transferencia internacional, sería necesario cumplir con estos requisitos para poder llevar a cabo dichas publicaciones. Esta exigencia traería como consecuencia inevitable la inutilización de la Red de Redes[2868]. Ayuda a llegar a la misma conclusión el hecho de que parece que el legislador, cuando se refiere a las transferencias internacionales, está regulando una operación en la que el receptor es un sujeto determinado, situado en un país concreto. Como se verá en los apartados siguientes, el concepto de transferencia internacional no abraza las revelaciones de datos cuando el destinatario es un sujeto indeterminado. Así, la publicación de datos vía Internet, en una simple página *web*, a un destinatario indefinido, no parece que pueda incardinarse en dicho concepto.

Es cierto que desde un punto de vista teórico puede llegar a discutirse la consideración que realiza el citado tribunal[2869]. La publicación de una información en Internet hace posible que estos datos puedan ser recogidos y manipulados en estados que no garantizan el derecho a la autodeterminación informativa de la misma manera que lo hace la Directiva europea o la LOPD en el ámbito interno[2870]. Y no se está haciendo referencia a países que tecnológicamente no han alcanzado el nivel de desarrollo que se ha logrado en el ámbito europeo o interno, sino a países

[2866] STJUE, 6 de noviembre de 2003, Bodi Lindqvist, asunto C-101/01, FJ 68. "Teniendo en cuenta, por un lado, el estado de desarrollo de Internet en el momento de la elaboración de la Directiva 95/46 y, por otro, la inexistencia, en su capítulo IV, de criterios aplicables al uso de Internet, no cabe presumir que el legislador comunitario tuviera la intención, en su momento, de incluir en el concepto de «transferencia a un país tercero de datos» la difusión de datos en una página web por parte de una persona que se encuentre en la misma situación que la Sra. Lindqvist, ni siquiera cuando dichos datos estén al alcance de personas de países terceros que disponen de los medios técnicos para poder acceder a ellos." BUISÁN GARCÍA, "Movimiento Internacional…", cit., 2008, p.572; BARCELÓ y PÉREZ ASINARI, "Transferencia Internacional…", cit., 2009, p. 145.

[2867] STJUE, 6 de noviembre de 2003, Bodi Lindqvist, asunto C-101/01, FJ 69: "Si el artículo 25 de la Directiva 95/46 se interpreta en el sentido de que existe una «transferencia a un país tercero de datos» cada vez que se publican datos personales en una página web, dicha transferencia será forzosamente una transferencia a todos los países terceros en los que existen los medios técnicos necesarios para acceder a Internet. El régimen especial que prevé el capítulo IV de la citada Directiva se convertiría entonces necesariamente, por lo que se refiere a las operaciones en Internet, en un régimen de aplicación general. En efecto, en cuanto la Comisión detectara, con arreglo al artículo 25, apartado 4, de la Directiva 95/46, que un solo país tercero no garantiza un nivel de protección adecuado, los Estados miembros estarían obligados a impedir cualquier difusión de los datos personales en Internet". GUERRERO PICÓ, *El Impacto de Internet...,* cit., 2006, p. 258.

[2868] DAVARA RODRÍGUEZ, "La Transferencia Internacional…", cit., 2006, p. 55.

[2869] COUDERT, "Transferencias Internacionales…", cit., 2007, p.459.

[2870] POULLET, "Flujos de Datos…", cit., 2006, pp. 99-100: critica la comentada STJUE, señalando que redes internacionales de espionaje, como puede ser ECHELON, conllevan operaciones de captación de datos que debían someterse a reglas más rigurosas que las que derivan de la interpretación realizada en la señalada sentencia.

como EEUU, que cuentan con unas garantías jurídicas más laxas en relación a este derecho[2871]. La publicación de unos datos en Internet hace posible que un tercero acceda a dicha información desde cualquier punto del planeta. El hecho de que los datos de salud de los ciudadanos puedan ser empleados en dichos estados no deja de generar cierta desconfianza e inseguridad. La asunción del concepto amplio de la transferencia internacional podría hacerse para dar garantías jurídicas suficientes a operaciones que, como la publicación, plantean un riesgo especial para el derecho a la autodeterminación informativa.

No cabe duda de que la publicación de unos datos en una página *web* constituye una transferencia, aunque no se trate por lo general de una transferencia dirigida a un destinatario en concreto[2872]. Sin embargo, desde el punto de vista práctico resulta complejo aceptar esta conclusión, pues haría prácticamente imposible la publicación de dato alguno de carácter personal en las incontables páginas *web* que configuran Internet[2873]. La transferencia parece exigir una acción de transmisión entre dos sujetos concretos. Con ello no se quiere concluir que este tipo de publicaciones no están sujetas a regla alguna. Como se ha dicho a la hora de analizar la figura de la cesión, una interpretación amplia de este concepto permite abrazar estas operaciones dentro de su ámbito de aplicación. Es cierto que la publicación por Internet de datos de carácter personal supone una transmisión. Por ello, tiene que cumplir con las exigencias que marca la normativa para la realización de cesión de datos o el cumplimiento del deber de secreto.

C) Al margen de estas puntualizaciones hay que señalar que la jurisprudencia ha ido considerando a lo largo del tiempo diferentes supuestos, que podrían ser dudosos, como transferencias internacionales de datos. Probablemente el caso más relevante es el siguiente. Si se atiende a las normas parece que el movimiento internacional se refiere a la relación entre un responsable o encargado situado en el estado y otro responsable o encargado situado en el extranjero. Se ha cuestionado por los órganos judiciales si hay una transferencia internacional cuando es el propio titular de los datos el que transmite la información de carácter personal a un país extranjero. En el caso concreto al que se enfrentaban los tribunales, una empresa española empleaba un sistema técnico por medio del cual los titulares de datos, que los entregaban para participar en un concurso, se veían compelidos, sin saberlo, a que sus datos personales quedaran reflejados en archivos de una entidad situada en los EEUU. Este servidor extranjero guardaba y manipulaba por cuenta de la empresa española esta información para después transmitirla otra vez a la entidad estatal, que volvería a tratar la información recabada en el extranjero a fin de organizar dicho concurso[2874].

En principio, y si se atiende a la equiparación que en el RDLOPD se realiza entre la transferencia internacional y la cesión, no parece que el caso citado pueda considerarse como

[2871] Memoria de la AEPD de 1995. Se pone de manifiesto que durante ese año se realizó un alto número de transferencias a EEUU, que tenían como base el hecho de que este país contaba con un nivel de protección adecuado. Ante esta situación se requirió a los responsables de los ficheros que llevaron a cabo estas operaciones que rectificaran ese error.
[2872] HEREDERO HIGUERAS, "La Transmisión Internacional…", cit., 2006, p. 194.
[2873] FERNÁNDEZ SALMERÓN y VALERO TORRIJOS, "La Difusión de Información Administrativa…", cit., 2005, p. 109
[2874] SAN 21 julio de 2004, FJ 2.

movimiento internacional. Parece que estos movimientos abrazan más bien la transmisión por parte de un responsable a otro sujeto y no la transmisión del propio titular a otra persona situada en el extranjero. Los tribunales, sin embargo, llevan a cabo en este caso una interpretación amplia del concepto de transferencia internacional para aplicar el régimen jurídico que les concierne a estas acciones en que se relacionan directamente el titular y otro sujeto. No se escapa aquí que esta interpretación viene motivada en este supuesto por las circunstancias que rodean al caso, fundamentalmente por el hecho de que el tratamiento se llevó a cabo sin la debida información y sin recabar el consentimiento de los titulares. Sin embargo, se entiende que el planteamiento de los órganos judiciales es correcto: "(…) tanto da que el mecanismo empleado haya sido la ubicación directa de los datos personales en el servidor extranjero por los propios afectados, -además, volvemos a repetir, sin su conocimiento y consentimiento- que los datos se hayan transmitido al extranjero, después de pasar por un servidor español, porque el resultado ha sido el mismo: los datos han llegado a conocimiento de una entidad ubicada en el extranjero"[2875]. Si bien en relación a Internet se ha llevado a cabo una interpretación restrictiva del concepto que se analiza, más por motivos prácticos que otra cosa, no se hace lo mismo en el supuesto concreto planteado por la jurisprudencia. En este caso no hay razón alguna para negar la interpretación amplia. Independientemente de que la transmisión al extranjero la haga el propio titular u otro sujeto, sea responsable del fichero o encargado, los riesgos que rodean a esta operación motivan que todas estas operaciones sean consideradas como transferencias internacionales a fin de que a todas ellas les sean aplicables las garantías recogidas en el régimen jurídico referente a dichos movimientos internacionales.

De todo lo dicho hasta ahora, parece que la transferencia internacional de datos hace referencia a un movimiento determinado en el que la información sale del ámbito de control de un sujeto situado en un país, para integrarse en el ámbito de control de otro sujeto determinado o determinable situado fuera de dicho país.

III.3. La necesidad de que en las transferencias se respeten los principios aplicables a todo tratamiento.

Como se verá en los próximos apartados, el ordenamiento configura un régimen jurídico aplicable a las transferencias internacionales en el que las transmisiones se realizarán de diferente forma atendiendo el país de destino o las circunstancias concretas en que éstas se den. La protección del derecho a la autodeterminación informativa en este tipo de operaciones se lleva a cabo, sin embargo, no sólo en base a lo que disponen las disposiciones que se refieren expresamente a los movimientos internacionales, sino que han de tenerse en cuenta los principios que rigen en toda manipulación de datos de carácter personal. La transferencia internacional constituye una operación más de tratamiento de datos. Como no podía ser de otra forma, los criterios dados cuando se han analizado los principios de calidad, el consentimiento o la información son aplicables también a este tipo de manipulaciones[2876].

[2875] SAN 21 julio de 2004, FJ 9.

[2876] ESTADELLA YUSTE, *La Protección…,* cit., 1995, p. 129; ÁLVAREZ RIGAUDIAS, "Transferencias internacionales…", cit., 2008, p. 503; BARCELÓ y PÉREZ ASINARI, "Transferencia Internacional…", cit., 2009, p. 142.

A pesar de que las disposiciones que regulan los movimientos internacionales de datos no hacen mención expresa a la forma en que han de aplicarse estos criterios a este tipo de tratamiento, la vigencia de los mismos queda patente en el ordenamiento. Como bien señalan la Directiva[2877], el reglamento que desarrolla la LOPD[2878] y la Instrucción de la AEPD[2879], la transferencia internacional ha de sujetarse a las garantías y principios reconocidos en la Ley orgánica y en el propio reglamento que la desarrolla[2880]. En este sentido, hay que destacar el principio de finalidad, los principios de proporcionalidad y veracidad ya comentados, el principio de seguridad, el derecho a ser informado, el derecho al consentimiento y el deber de notificar la transferencia al Registro correspondiente, tanto cuando se trata de ficheros públicos como privados. El análisis de estos principios en este apartado no presenta particularidades con respecto de lo que ya se ha dicho hasta ahora. Si embargo, merece la pena detenerse en unos puntos para aclarar algún aspecto que puede generar confusión. Cabe hacer alguna apreciación en relación al ejercicio de los derechos a otorgar el consentimiento y a recibir información.

A) De inicio, el derecho a consentir permanece plenamente vigente en estas operaciones. Excepto en los casos en que la Ley prevé una excepción, las transferencias deberán contar con el consentimiento del titular de los datos. Dichas excepciones serán, se entiende aquí, las previstas en el apartado dedicado en la LOPD a regular las cesiones. Necesariamente, dependiendo del tipo de dato, dicha autorización podrá ser tácita, o deberá ser expresa o, además de expresa, escrita.

Más allá de esta afirmación, la Ley otorga al consentimiento del titular una dimensión especial cuando se trata de llevar a cabo transferencias internacionales de datos. La Ley dispone que el régimen general que regula los movimientos internacionales no será de aplicación a las trasmisiones que se realizan con el consentimiento inequívoco del titular[2881]. Esto quiere decir, básicamente, que cuando medie consentimiento del titular, podrán remitirse datos de carácter personal a cualquier lugar, independientemente de la protección jurídica que se otorgue en el país de destino al derecho a la autodeterminación informativa, sin necesidad de someterse a controles específicos, como el requerimiento de la autorización del Director de la AEPD. Según parte de la doctrina este consentimiento será distinto al genérico consentimiento que justifica la

[2877] Considerando 60 Directiva 95/46/CE: "*Considerando que, en cualquier caso, las transferencias hacia países terceros sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembro en aplicación de la presente Directiva, y, en particular, de su artículo 8* (que regula el tratamiento de las categorías especiales de datos)".

[2878] Artículo 65 RDLOPD: "*La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento"*.

[2879] Norma segunda Instrucción de la AEPD 1/2000, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos: "*la transferencia internacional de datos no excluye de la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, conforme a su ámbito de aplicación, correspondiendo a la Agencia de Protección de Datos la competencia para verificar su cumplimiento"*. Informe jurídico 101/2003, de la AEPD.

[2880] Dictamen 5/2007 de la APDCat, en relación con la consulta planteada por un Ayuntamiento referente al movimiento internacional de datos personales del padrón municipal: "Visto que en el caso que se consulta resulta de aplicación la excepción del artículo 34.k) (…), no sería necesario el examen previo para la correspondiente autorización (…), aunque, evidentemente, será siempre preceptivo el cumplimiento de los principios y obligaciones que exige la legislación de protección de datos". DAVARA RODRÍGUEZ, *Manual de Derecho…,* cit., 2005, p. 108. SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 583.

[2881] Artículo 34.e) LOPD.

transferencia, y se otorgará específicamente con el fin de habilitar la excepción al régimen general[2882]. Siguiendo esta interpretación se requerirían, por lo tanto, dos consentimientos diferentes para justificar la transferencia: el otorgado para que la transmisión se lleve a cabo y el que se da para superar los requisitos exigidos por las normas. No se comparte aquí dicho argumento. Si el titular de los datos otorga el consentimiento para realizar la transferencia una vez ha sido informado sobre las características concretas de la operación, no parece que sea necesario un nuevo consentimiento, que no aportaría nada nuevo y que sólo llevaría a una excesiva burocratización de la operación. El consentimiento vendría en estos casos a sustituir el sistema de control que las normas establecen para que toda transferencia se realice con las máximas garantías. Como más adelante se verá, puede ser criticable el hecho de dejar en manos de los particulares esta posibilidad, sobre todo, debido al desconocimiento que pueden tener de los riesgos que implica una transferencia internacional en determinadas circunstancias. Es por ello que se entiende, que el consentimiento deberá ser fruto de un riguroso y completo ejercicio de información al titular de los datos.

B) En cuanto al derecho a ser informado sobre la transferencia que se pretende realizar, ni la Ley ni el reglamento que la desarrolla dicen nada al respecto. La comentada Instrucción de la AEPD reconoce la obligación del responsable de informar a los afectados por el tratamiento de la realización de la transmisión, salvo que la persona importadora fuera a actuar como mero encargado de tratamiento situado fuera del Estado[2883]. Sin embargo, la obligación de informar impuesta por esta norma fue puesta en duda por los tribunales, que llegaron a cuestionar su letra argumentando que "ningún apartado del mencionado artículo 5 de la Ley Orgánica establece de manera específica el deber de informar a los interesados sobre las transferencias internacionales de los datos que les afecten"[2884]. Podría cuestionarse, por lo tanto, si estas operaciones han de sujetarse a la obligación de informar al afectado al respecto.

Se entiende que la valoración de los tribunales es superficial, al partir de una interpretación literal especialmente restrictiva del precepto de la LOPD que citan. Si bien es cierto que no hay referencia alguna a las transferencias internacionales en el artículo 5 de la Ley que regula el derecho a ser informado, no se puede obviar que la disposición reconoce el derecho de los afectados por un tratamiento de datos a conocer quiénes serán "los destinatarios de la información"[2885]. No cabe duda de que quien se erige en importador en una transferencia internacional de datos no es otra cosa que un destinatario. Empleando argumentos de mayor calado, no parece que tenga sentido reconocer el derecho a la información cuando la operación a realizar es una cesión de datos y no hacerlo cuando se trata de una transferencia internacional,

[2882] SÁNCHEZ CARO y ABELLÁN, *Datos de Salud…,* cit., 2004, pp. 80-81

[2883] Norma segunda Instrucción de la AEPD 1/2000, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos: "*de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, cualquier responsable de un fichero o tratamiento que se proponga transferir datos de carácter personal fuera del territorio español deberá haber informado a los afectados de quiénes serán destinatarios de los datos, así como de la finalidad que justifica la transferencia internacional y el uso de los datos que podrá hacer el destinatario.*
El deber de información al que se refiere el párrafo anterior no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero, en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999".

[2884] SAN 15 de marzo de 2002, FJ 6.

[2885] Artículo 5.1.a) LOPD.

por mucho que la transmisión se realice a países que cuentan con un nivel adecuado de protección. Si se exige el cumplimiento del deber de informar cuando se trata de una cesión, que es una operación que se da en un ámbito más cercano, donde el control puede ser más sencillo, parece lógico que ese requerimiento tenga vigencia cuando el control efectivo sobre los datos puede resultar más complejo, caso de las transferencias de alcance internacional[2886]. Evidentemente, si el derecho a la autodeterminación informativa constituye el derecho a controlar lo que sucede con los datos de cada uno, parece obvio que la transmisión de dicha información más allá de las fronteras del Estado exigirá que el titular de los datos conozca dicho movimiento. Hay que tener en cuenta además que el derecho a ser informado constituye la base para el ejercicio del derecho a consentir el tratamiento y los derechos de acceso, de rectificación, de cancelación y de oposición. En la medida en que estos derechos tampoco han sido negados en estas operaciones no parece que el de información pueda exceptuarse.

Esta línea interpretativa parece compartir también el Grupo de Trabajo sobre protección de datos del artículo 29 de la Directiva. Este organismo reconoce el derecho a la información, no sólo cuando la transferencia se realiza entre dos responsables sino también cuando se da entre un responsable y un encargado situado fuera del Estado. Al contrario de lo que hacía la Instrucción de la AEPD, que excluía del deber de informar al afectado cuando el movimiento se producía entre un responsable y un encargado[2887], el Grupo de Trabajo advierte de la inoportunidad de esta exclusión, y entiende que, por lo menos en lo que se refiere a datos sensibles, los afectados serán informados de la transferencia internacional a países que no presentan un nivel adecuado de protección[2888]. Como se apuntara al hablar del acceso por cuenta de terceros, se entiende aquí que no sólo cuando se refiere a los datos sensibles, sino que en todo caso el deber de informar tiene que acompañar a esta operación, pues el afectado tiene derecho a conocer el destino de los datos que le conciernen incluso cuando el acceso a los datos por el encargado del tratamiento se hace por cuenta del responsable.

El derecho a la información está vigente en los movimientos internacionales de datos. Es más, debido a las especificidades que presenta este tipo de operación, en ocasiones será necesario que la información al afectado no se quede en los elementos a los que se refiere el artículo 5 de la Ley. Como se verá, cuando la transferencia requiere de una autorización del Director de la AEPD, por tratarse el país destinatario de un lugar que no cuenta con un nivel de protección adecuado, es necesario que se creen los mecanismos necesarios para que se garantice la salvaguarda del derecho a la autodeterminación informativa de los afectados. Entre

[2886] STS 28 de abril de 2009, FJ 6. Pone de manifiesto la importancia de que unos titulares de datos tengan conocimiento de que la información que les concierne ha sido manipulada en EEUU, a pesar de que la finalidad, desarrollar una campaña publicitaria, iba a ser cumplida en el Estado.

[2887] Norma segunda Instrucción 1/2000 de la AEPD, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos: el deber de información del artículo 5 de la LOPD *"no será de aplicación cuando la transferencia tenga por objeto la prestación de un servicio al responsable del fichero, en los términos establecidos por el artículo 12 de la Ley Orgánica 15/1999"*. SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 585.

[2888] Dictamen del Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE, 7/2001, de 13 de septiembre de 2001, relativo al Proyecto de Decisión de la comisión (versión 31 de agosto de 2001) sobre las Cláusulas Contractuales Tipo para la Transferencia de Datos Personales a Encargados del Tratamiento establecidos en Terceros Países, al amparo de los dispuesto en el apartado 4 de la Directiva 95/46.

esos mecanismos estará también el establecimiento de instrumentos a través de los que los afectados podrán exigir responsabilidades en caso de que haya habido una vulneración. Para que estos instrumentos puedan ser empleados los afectados deberán ser informados sobre los parámetros en los que se han llevado a cabo las transferencias. En este sentido, las diferentes Decisiones de la Comisión Europea que regulan las cláusulas contractuales tipo que se han de respetar para entender que una transferencia a un país que no guarda un nivel de protección adecuado pueda llevarse a cabo, subrayan la importancia de que se informe al interesado sobre la existencia y finalidad de las transferencias[2889].

III.4. Supuestos de movimiento internacional de datos.

El texto de la LOPD, parece partir de una consideración negativa de la transferencia internacional: "No podrán realizarse transferencias…" Ni la Directiva ni el Convenio de 1981 recogen esa perspectiva[2890]. Efectivamente, estos textos, al igual que el RDLOPD y la Instrucción de la AEPD, parten de otro punto de vista[2891]. Se podría decir que, si bien en el fondo la regulación de un texto normativo a otro no varía demasiado, de la redacción de dichos textos no se deduce ese cariz prohibitivo que se recoge en la Ley estatal. Parece que el legislador interno asume desde el inicio los riesgos de este tipo de operaciones y la necesidad de que las transferencias sólo puedan realizarse en determinadas circunstancias.

El ordenamiento recoge diferentes supuestos de transferencia internacional de datos. Fundamentalmente se distinguen tres tipos distintos. En primer lugar se encuentra la transmisión a países que presentan un sistema de protección equiparable al establecido en la LOPD. En segundo, la transferencia a países que no cuentan con ese nivel de protección. El ordenamiento dispone reglas o criterios diferentes a la hora de regular uno y otro supuesto, pero en ambos casos la normativa pretende que la transferencia se realice con unas mínimas garantías y, sobre todo, asegurar que, una vez los datos hayan sido transmitidos, éstos vayan a ser manipulados en un marco o entorno adecuado de protección. En tercer lugar, las normas recogen una serie de supuestos que quedan exceptuados del régimen general dispuesto para los dos casos anteriores y en los que las transferencias pueden realizarse con gran libertad.

No corresponde aquí realizar un estudio exhaustivo sobre las características de cada uno de los supuestos de transferencia internacional de datos. Bastará con apuntar los parámetros principales en que ha de realizarse cada una de las formas de transmisión para dibujar el marco en el que los datos sanitarios pueden ser comunicados a otros países.

[2889] Apéndice 2 Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a Cláusulas Contractuales Tipo para la Transferencia de Datos Personales a un Tercer País previstas en la Directiva 95/46/CE, en DO nº L-181/19, 4 de julio de 2001: "Se deberá facilitar a los interesados información sobre la finalidad del tratamiento y la identidad del responsable del tratamiento de los datos en el tercer país, así como cualquier otra información en la medida en que sea necesaria para garantizar el tratamiento leal, a menos que dicha información ya la haya proporcionado el exportador de datos".

[2890] Artículo 25.1 Directiva 95/46/CE: "*Los Estados miembros dispondrán que la transferencia a un país tercero (...) únicamente pueda efectuarse (...)*"; Artículo 12.2 Convenio 108/1981 del Consejo de Europa: "*Las disposiciones que siguen se aplicarán a las transmisiones a través de las fronteras nacionales, por cualquier medio que fuere, de datos de carácter personal (...)*". HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, pp. 316-317.

[2891] BUISÁN GARCÍA, "Movimiento Internacional…", cit., 2008, p. 555.

III.4.1. Transferencia de datos a un país con nivel de protección adecuado.

A continuación se analizará el primer supuesto de transferencia internacional, que no es otro que el que se puede dar a países que proporcionan un nivel de protección de datos equiparable al reconocido en el sistema jurídico español. La importancia de determinar cuáles son estos estados reside en que la información podrá fluir entre ellos sin necesidad de cumplir con estrictas medidas de control.

III.4.1.A. Definición de los criterios para determinar si un país cuenta con un nivel de protección adecuado.

La LOPD señala que las transferencias a países que no presentan un nivel de protección equiparable al configurado en el ámbito interno requerirán de la autorización del Director de la AEPD, que la otorgará una vez se haya verificado que existen garantías suficientes para realizar dicha operación[2892]. Una lectura *a sensu contrario* de lo que dispone la norma da a entender, que a los países que presentan un nivel equiparable de protección pueden llevarse a cabo transferencias sin necesidad de autorización específica de la Agencia de Protección de Datos, en principio, con plena libertad[2893]. El principal efecto de la consideración de un Estado como portador de un sistema de protección adecuado es la posibilidad de realizar las transferencias a dicho país sin la obligación de sujetarse a un riguroso sistema de control previo. El sistema de control minorado al que se someten este tipo de movimientos será analizado más adelante. Interesa ahora determinar qué países cuentan con esta consideración privilegiada y definir el criterio que se sigue para considerar que un Estado guarda un sistema de protección adecuado.

Antes de dar respuesta a estas dos cuestiones es necesario aclarar la confusión que puede generar el uso aleatorio que se realiza en la Ley de los conceptos equiparable y adecuado[2894]. En los preceptos dedicados en esta norma a regular los movimientos internacionales de datos se utilizan indistintamente los conceptos “equiparable” y “adecuado”, y se hace mención también a las “garantías adecuadas”. El RDLOPD también utiliza en algún caso el concepto “equiparable” junto al de “adecuado”[2895]. La Directiva en todo momento emplea el término “adecuado”. Por su parte, el Convenio de 1981 sobre protección de datos utiliza el de “equivalente”[2896]. Evidentemente, no es lo mismo “equiparable” y “adecuado”. Lo primero hace referencia a algo “igual o equivalente” y lo segundo a algo “apropiado a las condiciones, circunstancias…”[2897]. De inicio, parece que lo equiparable plantea mayores exigencias, pues requiere que algo sea igual a un modelo determinado, en este caso, a las garantías a aplicar en la protección del derecho a la

[2892] Artículo 33.1 LOPD.
[2893] COUDERT, “Transferencias Internacionales…”, cit., 2007, p. 431.
[2894] ESTADELLA YUSTE, *La Protección…,* cit., 1995, p. 117.
[2895] Artículo 67.2 RDLOPD.
[2896] Artículo 12.3 Convenio 108/10981 del Consejo de Europa. Si bien el Protocolo Adicional al Convenio, hecho en Estrasburgo el 8 de noviembre de 2001 y ratificado por España en BOE 20 de septiembre de 2010, emplea también el término “adecuado”.
[2897] http://www.rae.es/

autodeterminación informativa[2898]. En cambio lo adecuado no exige esa igualdad, sino que bastará con que se cumplan unas determinadas condiciones[2899].

El uso indistinto que se hace en la Ley de ambos términos podría llevar a entender que la transmisión realizada a países que ofrecen un nivel equiparable de protección y la llevada a cabo a países que cuentan con un nivel de protección adecuado constituyen supuestos diferentes de transferencia, que exigen requisitos distintos[2900]. La equiparabilidad podría hacer referencia a la necesidad de realizar un ejercicio comparativo ente las normas dirigidas a regular la protección de datos. La adecuación, en cambio, como se recoge en todas las normas, se referiría a criterios más heterogéneos: circunstancias, condiciones, etc.

Esta distinción no parece que tenga aplicación real en las normas. Si se realiza una interpretación conjunta de la Ley, el reglamento que la desarrolla y la Directiva europea, se verá que en realidad lo equiparable y lo adecuado se emplean como sinónimos. La norma europea no utiliza el término equiparable, mientras que el reglamento, si bien lo utiliza en alguna ocasión, configura el régimen jurídico a aplicar a las transferencias internacionales sobre el concepto adecuado. Es más, el enunciado del capítulo concerniente a este tipo de transmisiones se refiere a las "Transferencias a Estados que proporcionen un Nivel Adecuado de Protección".

En definitiva, se entenderá que el primer supuesto de transferencia internacional se refiere a las transmisiones que se realizan a países que proporcionan un nivel adecuado de protección. Tiene sentido esta interpretación por cuanto que, tanto en la LOPD como en la Directiva y el RDLOPD, los factores a los que habrá que atender para determinar si un Estado ofrece un nivel de protección adecuado se corresponden con los que se han citado en la definición dada sobre el concepto "adecuado": circunstancias, condiciones, etc. En cualquier caso, no se puede interpretar que en la práctica el empleo del término adecuado constituya una minoración de las garantías a exigir en comparación al término equiparable. Se entiende aquí que, teniendo en cuenta que cuando se considera que un país presenta un nivel de protección adecuado las transferencias podrán realizarse con relativa libertad, la determinación de un régimen jurídico de protección de datos como adecuado ha de responder a criterios igualmente exigentes a los que derivarían del empleo del término equiparable[2901].

Los requisitos para determinar si un nivel de protección es adecuado se establecen en la LOPD en el artículo 33.2. Si se cumplen estas exigencias la transmisión podrá darse sin necesidad de autorización del Director de la AEPD. La distribución de los preceptos en la redacción de la Ley genera cierta confusión a la ahora de determinar si estos criterios son aplicables a este tipo de transferencias o a las que requieren de autorización del Director de la AEPD. El apartado primero del artículo 33 dispone que cuando un régimen jurídico no establece

[2898] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 178; COUDERT, "Transferencias Internacionales…", cit., 2007, p. 430.
[2899] BUISÁN GARCÍA, "Movimiento Internacional…", cit., 2008, p. 568.
[2900] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 367.
[2901] HEREDERO HIGUERAS, *La Directiva...*, cit., 1997, pp. 187-188, apunta que "la doctrina ha preferido la noción de <<nivel de protección adecuado>> frente a la de <<protección equivalente>>, por estimar que (...) la noción de nivel de protección adecuado es más realista y en la práctica será más efectiva que la imposición de una obligación rigurosa de los Estados miembros de no transferir sino a Estados terceros con protección equivalente".

un sistema de protección adecuado será necesaria una autorización del Director de la AEPD para que la transferencia internacional pueda realizarse. Esta autorización se dará una vez se haya constatado que existen "garantías adecuadas" para ello. El apartado segundo de dicho artículo comienza señalando que el "carácter adecuado (…) se evaluará (…)". Podría parecer que el artículo 33.2 se refiere a las citadas garantías adecuadas que han de analizarse para otorgar la pertinente autorización. Es decir, podrían confundirse los conceptos de "garantías adecuadas" que son necesarias para otorgar la citada autorización y el concepto de "nivel de protección adecuado", que cuando es alcanzado por un país las transferencias al mismo no exigen de autorización alguna. La confusión se aclara en el texto del RDLOPD[2902], que señala expresamente que los criterios fijados en el artículo 33.2 de la Ley hay que vincularlos con la consideración de un sistema de protección de datos como adecuado, no con la determinación de una transferencia concreta como sujeta a garantías adecuadas a efectos de que sea autorizada.

Disponen la LOPD y el reglamento que la desarrolla, que en este punto reproducen lo dispuesto por la Directiva europea[2903], que para analizar si efectivamente el país de destino presenta un nivel de protección adecuado, habrá que tener en cuenta "*(…) todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*"[2904].

Como se observa, hay que atender a diversos aspectos para determinar el nivel de protección que el país de destino otorga a los datos de carácter personal. El Grupo de Trabajo del artículo 29 ha aclarado el sentido de estos requisitos distinguiendo dos bloques[2905]. Por un lado habrá que tener en cuenta los principios de contenido. Para asegurarse de que un sistema de protección de datos es adecuado hay que tomar en consideración si en dicho régimen se guardan los principios fundamentales de protección de datos: los relativos a la calidad, el derecho a ser informado, el principio de seguridad, los derechos de acceso, cancelación, rectificación y oposición, y si se establecen restricciones a futuras transferencias a países terceros. Por otro, habrá que atender a si se establecen mecanismos suficientes que garanticen la aplicación de dichos principios: hay que valorar, fundamentalmente, el sistema utilizado para asegurar la eficacia de las normas de protección de datos, atendiendo a si en la práctica en el país de destino se cumplen los principios citados, si se asiste al afectado, si existe una entidad

[2902] Artículo 67.1 RDLOPD, en el que se vinculan expresamente los citados criterios a las Transferencias a Estados que proporcionen un Nivel Adecuado de Protección.
[2903] Artículo 25.2 Directiva 95/46/CE.
[2904] Artículo 33.2 LOPD.
[2905] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre la transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, 24 de julio de 1998. Este sistema se ha empleado en la consideración de sistemas de protección de datos concretos como en el Dictamen 6/2003 del Grupo de Trabajo del artículo 29, relativo al nivel de protección de los datos personales en la Isla de Man, 21 de noviembre de 2003.

independiente que garantice el cumplimiento de las normas y si hay vías de recurso adecuadas para poder exigir responsabilidades.

De los criterios establecidos llama la atención la cita que se hace en los textos jurídicos a las normas profesionales. Como se pone de manifiesto en todos ellos, la protección no tiene que venir necesariamente por las leyes sino que puede venir de mecanismos de autorregulación. La cita a las normas profesionales, constituye una clara referencia a las reglas de autorregulación entendidas por el citado Grupo de Trabajo como el "conjunto de normas de protección de datos aplicable a una pluralidad de responsables del tratamiento que pertenezcan a la misma profesión o al mismo sector industrial, cuyo contenido haya sido determinado fundamentalmente por los miembros del sector industrial o profesión en cuestión"[2906]. El empleo de esta técnica como garantía de un adecuado nivel de protección de los datos de carácter personal ha venido reforzado por diferentes textos del Grupo de Trabajo del artículo 29, que han dado mayor margen de actuación a normas de autorregulación, como las denominadas *Binding Corporate Rules,* que constituyen reglas corporativas vinculantes y que tienen aplicación fundamentalmente en el ámbito empresarial[2907]. Se ha considerado que este tipo de reglas pueden configurar mecanismos determinantes a la hora de considerar que un sistema de protección de datos presenta un nivel adecuado de garantías. El principal problema que plantea este tipo de regulación es el asegurar que haya garantías de cumplimiento de dichas normas, pues se trata de reglas de autorregulación, como códigos tipo, que no tienen *per se* la fuerza vinculante que posee una ley. Evidentemente, el establecimiento de garantías suficientes pasa también porque se fije un mecanismo para que, en caso de violación de algún derecho, se pueda reclamar la responsabilidad a que hubiere lugar.

III.4.1.B. La determinación de los estados que se considera respetan un nivel de protección adecuado.

La determinación de los Estados que se considera contienen un nivel de protección adecuado al de la normativa estatal de protección de datos correspondía, en principio, al Ministerio de Justicia e Interior, como ponía de manifiesto el reglamento que desarrollaba la LORTAD[2908]. En base a este precepto se emitieron en 1995 y 1998 dos órdenes que determinaban la relación de

[2906] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre la transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, 24 de julio de 1998.

[2907] *Working document: transfer of personal data to third countries: applying article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for international data transfer,* de 3 de junio de 2003; *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules,* 24 junio de 2008; *Working Document Setting up a Framework for th estructure of Binding Corporate Rules,* 24 de junio de 2008. *Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 24 de junio de 2008. CERVERA NAVAS, "Primera Aproximación...", 2003; GARDAIN, "Transferencia de datos personales a países terceros…", cit., 2005; SANCHO VILLA, "Normas Corporativas…", cit., 2008, pp. 35-61, da un repaso general a la problemática que plantean estas normas corporativas vinculantes.

[2908] Disposición Final primera RD 1332/1994, 20 de junio de 2004, por el que se Desarrollan Algunos Puntos de la LORTAD: "*Lista de países con equiparable protección.- Se faculta al Ministro de Justicia e Interior para que, previo informe del Director de la Agencia de Protección de Datos, apruebe la relación de países que, a efectos de lo dispuesto en el artículo 32 de la Ley Orgánica 5/1992, se entiende que proporcionan un nivel de protección equiparable al de dicha Ley".* En este sentido también se pronuncia APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, pp. 187-189

países con protección de datos equiparable a la española[2909]. Sin embargo, la AEPD, una vez entró en vigor la LOPD, interpretó en un informe jurídico posterior de especial relevancia[2910], que el Ministro de Justicia e Interior era incompetente para la fijación de esta lista, debido a que dicha Ley en su artículo 33.2 remite a la AEPD la competencia para determinar el nivel adecuado de protección de los diferentes Estados[2911]. Hoy día, la LOPD y el reglamento que la desarrolla no dejan lugar a dudas: corresponde a la Agencia determinar si un país guarda un nivel adecuado de protección a través de una resolución administrativa, que deberá ser publicada en el BOE[2912].

La consideración de que un país mantiene un nivel de protección adecuado la puede realizar, además de la AEPD, la Comisión de la Unión Europea. Tanto la LOPD[2913], como el reglamento[2914] disponen que este último organismo cuenta con plena capacidad para decidir que un país guarda un nivel de protección adecuado. Sin embargo, el planteamiento realizado por ambas normas sobre el papel de la Comisión en este sentido es sustancialmente distinto. En la Ley interna se entiende que las transferencias realizadas a los países que determina la Comisión como portadores de un sistema de protección adecuado quedan exceptuadas del régimen general aplicable a los movimientos internacionales. La Ley los engloba en el apartado de las excepciones. Por el contrario, en el reglamento que desarrolla la LOPD estas mismas transferencias entran en el ámbito de aplicación del citado régimen general, siéndoles de aplicación las reglas que regulan los movimientos de datos a los países que cuentan con un nivel de protección adecuado, con los efectos que ello conlleva. El efecto principal sería la posibilidad de suspender por parte del Director de la AEPD esas transferencias si se dan una serie de circunstancias[2915]. En aplicación rigurosa de la Ley orgánica esta posibilidad de aplicar la suspensión resultaría dudosa, al estar este tipo de transferencias exceptuadas de la aplicación del régimen general. La solución a esta contradicción pasa por la lectura de la Directiva europea. En esta norma la transmisión de datos de carácter personal a países que han sido considerados por la Comisión Europea como portadores de un nivel de protección adecuado se incluye en el régimen general regulador del movimiento internacional de datos[2916]. Es así que, ante la duda

[2909] Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995, por la que se aprueba la primera relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE nº 35, 10 de febrero de 1995. Orden del Ministerio de Justicia e Interior de 31 de julio de 1998, por la que se amplía la relación de países con protección de datos de carácter personal equiparable a la española, a efectos de transferencia internacional de datos. BOE nº 200, 21 de agosto de 1998.

[2910] Informe jurídico AEPD, "Vigencia de la Orden del Ministerio de Justicia e Interior de 2 de febrero de 1995", 2002.

[2911] BUISÁN GARCÍA, "Movimiento Internacional…", cit., 2008, p. 557.

[2912] Artículo 67 RDLOPD: "*1. (...) Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el <<Boletín Oficial del Estado>>.*
2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.
Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos".

[2913] Artículo 34.k) LOPD.

[2914] Artículo 68 RDLOPD: "*No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección*".

[2915] Artículo 69 RDLOPD.

[2916] Artículo 25.6 Directiva 95/46/CE: "*La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo (...)*".

generada en el ámbito interno, hay que considerar la interpretación llevada a cabo por el reglamento que desarrolla la LOPD como la más adecuada.

La previsión de que las transferencias a los países definidos por la Comisión como portadores de un sistema adecuado de protección se integran en el ámbito de aplicación del régimen general que regula los movimientos internacionales, fundamentalmente la posibilidad de suspensión, lleva aquí a preguntarse, otra vez, porqué no se emplea la misma fórmula con las transmisiones a los países del Espacio Económico Europeo. Hay que recordar que los movimientos de datos realizados en este ámbito son considerados en el RDLOPD meras cesiones y no transferencias internacionales. Pues bien, si se tiene en cuenta que, al igual que ocurre con las transmisiones a los países que guardan un nivel de protección adecuado pero que no pertenecen al Espacio Económico Europeo, en las transferencias dentro del citado entorno se pueden dar los riesgos que justifican una suspensión de una transmisión, no se entiende porqué se otorga a este tipo de transferencias una consideración tan privilegiada.

En el marco jurídico actual se entiende que cabe realizar una transferencia internacional, sin necesidad de autorización alguna del Director de la AEPD, en el siguiente entorno: en primer lugar en los Estados miembros de la Unión Europea. En la medida en que se obligan a incorporar la Directiva a sus ordenamientos, se entiende, lógicamente, que para transmitir datos de carácter personal a cualquiera de estos países no hace falta autorización específica alguna de la Agencia de Protección de Datos, pues está garantizada la protección del derecho a la autodeterminación informativa en la propia normativa del Estado receptor. En este sentido, corresponde al Grupo del Artículo 29 de la Directiva europea comprobar la existencia de divergencias entre la legislación y la práctica de los Estados miembros que pudieren afectar a la equivalencia de la protección de las personas en lo que se refiere al tratamiento de datos personales en la Unión, informando de ello a la Comisión[2917]. A estos países hay que añadirles, los que componen el Espacio Económico Europeo que no pertenecen a la UE, tal y como recoge el reglamento que desarrolla la LOPD[2918]: Noruega, Islandia y Liechtenstein, y los que han ratificado el Convenio 108 del Consejo de Europa[2919]. Hay que sumarles, además, los que ha entendido la Comisión Europea que mantienen un adecuado nivel de protección. Así, Suiza[2920], Hungría[2921], las entidades que en EEUU respetan los denominados Principios de Puerto Seguro[2922], Argentina[2923], Guernsey[2924], la Isla de Man[2925] y Canadá[2926].

[2917] Artículo 30.2 Directiva 95/46/CE.
[2918] Memória de la AEPD, 2004.
[2919] Países como Croacia, Albania o Bosnia Herzegovina. ÁLVAREZ RIGAUDIAS, "Transferencias internacionales…", cit., 2008, p. 500.
[2920] Decisión de la Comisión Europea, 2000/518/CE, de 26 de julio del 2000. DO nº L-215, 25 de agosto de 2000.
[2921] Decisión de la Comisión Europea, 2000/519/CE, de 26 de julio del 2000. DO nº L-215, 25 de agosto de 2000. Siendo Hungría miembro de la UE desde 2004, hoy día no hay duda sobre la aplicación de un régimen flexible en la regulación de las transferencias de datos a este país.
[2922] Decisión de la Comisión Europea, 2000/520/CE, del 26 de julio del 2000. DO nº L-215, 25 de agosto de 2000.
[2923] Decisión de la Comisión Europea, 2003/490/CE, de 30 de junio de 2003. DO nº L-168, 5 de julio de 2003.
[2924] Decisión de la Comisión Europea, 2003/821/CE, de noviembre de 2003. DO nº L-308, 25 de noviembre de 2003.
[2925] Decisión de la Comisión Europea, 2004/411/CE, de 28 de abril de 2004. DO nº L-151, 30 de abril de 2004.

Hay que realizar un apunte sobre la problemática que plantean los denominados Principios de Puerto Seguro y las Preguntas más Frecuentes sobre los mismos. Estos principios constituyen criterios que garantizan que las entidades que los asumen mantienen un nivel adecuado de protección de los datos de carácter personal. Como se ha dicho más arriba, el marco jurídico estadounidense dirigido a salvaguardar el derecho a la autodeterminación informativa de las personas es muy diferente al que presenta la UE[2927]. Se trata de un marco sectorial, fundamentado en una mezcla de legislación, reglamentación y autorregulación[2928], que no alcanza *per se* a configurar un nivel de protección adecuado en relación al nivel existente en el ámbito de la UE y que hace imposible que se asuma una habilitación generalizada de transmisión de datos de carácter personal a los EEUU[2929]. La posibilidad de transmitir estos datos a un sujeto situado en este espacio territorial pasa porque el importador asuma unos principios que garanticen una protección adecuada de los datos de carácter personal y que, en lo básico, recojan las garantías que presenta el ordenamiento de la Unión. Desde 1999 el Grupo de Trabajo del artículo 29 ha emitido numerosos informes referentes a esos instrumentos. Desde el inicio se ha puesto de manifiesto que la principal preocupación en relación a esta cuestión la constituye la existencia de mecanismos que obliguen al cumplimiento de dichos principios y que garanticen la protección de los titulares de los datos en caso de que estos se incumplan[2930]. A lo largo, fundamentalmente, de ese año se han ido depurando los contenidos de dichos principios y de las "preguntas más frecuentes" realizadas al respecto, que entran también en el contenido de dichos principios[2931], hasta considerar en la actualidad que cumplen con un sistema adecuado de

[2926] Decisión de la Comisión Europea, 2002/02/CE, 20 de diciembre de 2001. DO nº L-02, 4 de enero de 2002. Se establecen matices sobre la posibilidad de transferir datos a importadores situados en Canadá, dependiendo de si se trata de sujetos sometidos a la *Personal Information and Electronic Documents Act* o no.

[2927] SANCHO VILLA, *Negocios Internacionales…*, cit., 2010, pp. 121-122.

[2928] DUMORTIER y GOEMANS, "Marcos para...", cit., 2000, "la filosofía de la reglamentación de los EEUU se basa más en una filosofía de intervención mínima por parte del estado. Para minimizar las intromisiones del estado en los flujos de la información, los Estados Unidos plantean la reglamentación del tratamiento de los datos personales más bien a través de la atención a la actividad sectorial y subsectorial diferenciada. Una ley amplia es muy poco frecuente".

[2929] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/9999, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos, 26 de enero de 1999.

[2930] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/1999, relativo al nivel de protección de datos en Estados Unidos y a los debates en curso entre la Comisión Europea y el Gobierno de Estados Unidos, 26 de enero de 1999. Proyecto de documento de trabajo, del Grupo de Trabajo del artículo 29, sobre el funcionamiento del acuerdo de puerto seguro, 2 de julio de 2002. COUDERT, "Transferencias Internacionales…", cit., 2007, p. 436.

[2931] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/1999, relativo a la idoneidad de los "Principios internacionales de puerto seguro" que hizo públicos el Departamento estadounidense de Comercio el 19 de abril de 1999, 3 de mayo de 1999; Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/1999, relativo a las "preguntas más frecuentes" que hará públicas el Ministerio de Comercio de los EEUU, en relación con la propuesta de "Principios de Puerto Seguro", 7 de junio de 1999; Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el estado del bate entre la Comisión Europea y el Gobierno de los Estados Unidos acerca de los "Principios internacionales de puerto seguro", 7 de julio de 1999; Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 7/1999, relativo a el nivel de protección de datos previsto por los principios de "puerto seguro" hechos públicos, junto con las preguntas más frecuentes y otros documentos relacionados, el 15 y 16 de noviembre de 1999 por el Departamento de Comercio de los EEUU, 3 de diciembre de 1999; Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 3/2000, sobre el diálogo entre la UE y los EEUU, acerca del Acuerdo de "Puerto Seguro", 16 de marzo de 2000; Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2000, sobre el nivel de protección que proporcionan los "Principios de Puerto Seguro", 16 de mayo de 2000.

garantía[2932]. No se puede dejar de apuntar aquí el principal problema que plantean los Principios de Puerto Seguro. La Comisión Europea considera que los organismos que se sujeten a los Principios de Puerto Seguro presentan un nivel de protección adecuado, por lo que las transferencias a dichos entes no requerirán de autorización, en el caso español, del Director de la AEPD. Esta situación lleva a que, la mayoría de las veces, el control sobre cómo se están manipulando los datos sólo podrá realizarse *a posteriori,* en caso de que haya alguna queja por parte de los titulares de los datos. En un sistema tan flexible como el propuesto por los citados principios, en el que la sujeción a dichos criterios es voluntaria, es necesario crear mecanismos que garanticen, de inicio, que en el país receptor se vayan a cumplir los niveles mínimos de protección.

El sistema fijado por el ordenamiento para determinar qué país presenta un nivel de protección del derecho a la autodeterminación informativa adecuado podría llegar a generar un problema de envergadura. Más allá de los supuestos en que es la Comisión Europea la que concluye la consideración de un país como portador de un sistema de protección adecuado, cuando son los propios Estados miembro los que llevan a cabo esa tarea puede ocurrir que un mismo país acabe teniendo consideraciones diferentes sobre su aptitud para ser destinatario de datos. La valoración a realizar por distintos países, dentro de la UE fundamentalmente, sobre el sistema de protección que presenta un Estado podría ser diferente. Esta situación generaría un desajuste en el flujo de información que se pretende crear con esta fórmula. Para evitar esta circunstancia la propia Directiva recoge mecanismos de información entre los países y la Comisión. En primer lugar obliga a todos los Estados miembros a que informen a la Comisión y a los demás estados sobre la consideración del régimen de protección de un país como adecuado, para que, en caso de que haya divergencias de criterios en torno a dicha conclusión puedan adoptarse las medidas oportunas[2933]. En segundo lugar establece un sistema por el que la Comisión pueda comprobar la situación de la protección del citado derecho en un país determinado y obrar en consecuencia, para que los Estados miembro eviten transferencias a dicho país[2934].

[2932] Estos principios se recogen en la Decisión 2000/520/CE, de la Comisión de 26 de julio de 2000, con arreglo a la Directiva 95/ 46/CE del Parlamento Europeo y del Consejo, sobre la Adecuación Conferida por los Principios de Puerto Seguro para la Protección de la Vida Privada y las correspondientes Preguntas más Frecuentes Publicadas por el Departamento de Comercio de Estados Unidos de América, DO nº L-215, 25 de agosto del 2000. Puede verse un interesante estudio sobre la aplicación práctica de los Principios de Puerto Seguro en DHONT, PÉREZ ASINARI, POULLET (con la asistencia de REIDENBERG y BYGRAVE), *Safe Harbour...,*cit., 2004, en http://www.europa.eu.int/. Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 4/2000, sobre el nivel de protección que proporcionan los "principios de puerto seguro", 16 de mayo de 2000. SAN 3 de noviembre de 2004, FJ 4. En la que se pone de manifiesto que una empresa estadounidense, a pesar de que cumple con una serie de medidas de seguridad, al no cumplir con los Principios de Puerto Seguro, no puede incardinarse en el ámbito de aplicación de la excepción del artículo 34.k) LOPD. Ocurre algo parecido en la SAN 21 de julio de 2004, FJ 9.

[2933] Artículo 26.3 Directiva 95/46/CE: "*Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.*
En el supuesto de que otro Estado miembro o la Comisión expresaran su oposición y la justificación debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de la persona, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".

[2934] Artículo 25.3 Directiva 95/46/CE: "*Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que se consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2".*

La consideración de un Estado como portador de un sistema de protección de datos adecuado es especialmente relevante. Entre los citados países se crea un espacio en el que los datos pueden circular con cierta libertad, sin ser sometido a controles previos rigurosos. Para realizar transferencias en este ámbito no es necesaria la autorización específica de las autoridades de control como la AEPD. Más allá de que, como es lógico, se tengan que cumplir con los requisitos que exige la Ley para realizar un tratamiento de datos, información, consentimiento, notificación, etc., los datos pueden fluir con libertad en este entorno.

III.4.1C. Los sistemas de información en el marco de Schengen, Eurojust y Europol como ejemplos del libre flujo de datos en el ámbito de la UE.

A pesar de que las transmisiones dentro del ámbito de la UE no son consideradas en el RLDOPD como transferencias internacionales, es significativo, como ejemplo de lo expuesto hasta ahora, el flujo de información que diferentes sistemas de información en este espacio territorial han creado, con el objetivo de controlar la circulación de los ciudadanos en dicho entorno y de combatir la delincuencia que afecta a más de un Estado miembro. Se está haciendo referencia fundamentalmente a los sistemas de información configurados en aplicación de los acuerdos en relación a Schengen, Eurojust y Europol. Cierto es que estos instrumentos quedan fuera del ámbito de aplicación de la Directiva europea sobre protección de datos, pues ésta no tiene aplicación en el ámbito del Segundo y Tercer Pilar, caso del tratamiento de datos para combatir el terrorismo[2935]. Sin embargo, los propios textos que regulan estos espacios, conscientes de la importancia que tiene el tratamiento de los datos de carácter personal en los mismos, realizan remisiones principalmente al Convenio de 1981[2936]. Como no podía ser de otra manera, la manipulación de datos de carácter personal que se crea en aplicación de estos acuerdos deberá realizarse con las garantías que ésta prevé, incluidas las relativas a las transferencias internacionales de datos. Evidentemente, los datos de carácter personal deben estar disponibles para alcanzar fines como la seguridad pública o combatir la delincuencia organizada. No obstante, estos tratamientos han de realizarse también de forma respetuosa con el derecho a la autodeterminación informativa. En esta línea, se aprobó en el entorno de la UE la

Artículo 25.4 Directiva 95/46/CE: "*Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate*".
Artículo 25.5: "*La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4*".
Artículo 25.6: "*La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas.*
Los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".

[2935] Artículo 3.2 Directiva 95/46/CE: "*Las disposiciones de la presente Directiva no se aplicarán al tratamiento de datos personales: -efectuado en el ejercicio de actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos V y VI del Tratado de la Unión Europea y, en cualquier caso, al tratamiento de datos que tenga por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dicho tratamiento esté relacionado con la seguridad del Estado) y las actividades del Estado en materia penal (...)*". PIÑAR MAÑAS, "Protección de dato…", cit., 2009, p. 153.

[2936] HEREDERO HIGUERAS, "La Transmisión Internacional…", cit., 2006, p. 203.

Decisión Marco del Consejo relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, en la que se prevé la posibilidad de transmitir datos sensibles entre diferentes estados para el cumplimiento de los objetivos citados, cuando sea estrictamente necesario[2937].

El acuerdo de Schengen entró en vigor en España en 1991[2938]. Este acuerdo tiene como finalidad principal el control de los ciudadanos que circulan entre los estados contratantes, fundamentalmente de extranjeros y personas que pueden constituir objeto de interés policial o judicial. El Convenio de aplicación de dicho acuerdo crea el "Sistema de Información Schengen (SIS)" con el fin de que haya un flujo eficiente de información que permita llevar a cabo dicho control[2939]. Ya en este texto se hacen constantes remisiones a lo que dispone el contenido del Convenio de 1981 sobre protección de datos[2940]. El último exponente del SIS es la creación del SIS II, que constituye un sistema más avanzado de flujo de información[2941] y que viene a sustituir al primero[2942]. En principio se niega la posibilidad de manipular en ese sistema de información datos que tienen la consideración de sensibles, caso de los sanitarios[2943]. El miedo de que este sistema de información pueda ser empleado de manera sistemática, como un medio de control general de los ciudadanos, y no como un instrumento cuyo uso ha de estar justificado en cada caso ha sido puesto de manifiesto por el Grupo de Trabajo del artículo 29[2944].

[2937] Artículo 6, Decisión Marco 2008/977/JAI del Consejo, 27 de noviembre de 2008, relativa a la protección de datos tratados en el marco de la cooperación policial y judicial en materia penal. BAYO DELGADO, "Los artículos 22, 23…", cit., 2010, p. 1.344 y siguientes.

[2938] Protocolo de Adhesión de 25 de junio de 1991 del Gobierno del Reino de España al Acuerdo entre los gobiernos de los estados de la Unión Económica Benelux, de la república federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 14 de junio de 1985, en 25 de junio de 1991, BOE nº 181, 30 de julio de 1991.

[2939] Artículo 92 y siguientes del Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, 19 de junio de 1990.

[2940] Artículos 94, 115 y 117 Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, 19 de junio de 1990. MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información…,* cit., 2001, p. 277; ULL PONT, *Derecho Público…,* cit., 2003, p. 63; ACED FÉLEZ, "La protección de datos…", cit., 2010, pp. 1.362 y siguientes.

[2941] Reglamento del Parlamento Europeo y del Consejo 1987/2006, 20 de diciembre de 2006, relativo al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SISII), DO nº 381, 28 de diciembre de 2006; y Decisión del Consejo 2007/533/JAI, 12 de junio de 2007, relativa al establecimiento, funcionamiento y utilización del Sistema de Información de Schengen de segunda generación (SISII), DO nº L-205/63, 7 de agosto de 2007.

[2942] Reglamento (CE) n o 1104/2008 del Consejo, de 24 de octubre de 2008 , sobre la migración del Sistema de Información de Schengen (SIS 1+) al Sistema de Información de Schengen de segunda generación (SIS II), DO nº L-299/1, 8 de noviembre de 2008; y la Decisión del Consejo 2008/839/JAI, 24 de octubre de 2008, sobre la migración del Sistema de Información de Schengen (SIS 1 +) al Sistema de Información de Schengen de segunda generación (SIS II), DO nº 299/43, 8 de noviembre de 2008. ACED FÉLEZ, "La protección de datos…", cit., 2010, pp. 1.377 y siguientes.

[2943] Artículo 94 Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, 19 de junio de 1990: "*(...) No se autorizarán otras anotaciones, en particular los datos enumerados en la primera frase del artículo 6 del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas en lo referente al tratamiento informatizado de datos de carácter personal*".

[2944] Dictamen 6/2005 sobre las propuestas de Reglamento del Parlamento Europeo y del Consejo (COM (2005) 236 final) y de Decisión del Consejo (COM (2005) 230 final) sobre el establecimiento, funcionamiento y utilización del Sistema de Información Schengen de segunda generación (SIS II) y sobre una propuesta de Reglamento del Parlamento Euopeo y del Consejo relativo al acceso al Sistema de Información Schengen de segunda generación (SIS II) por los servicios de los Estados miembro responsables de la expedición de los certificados de matriculación de vehículos (COM (2005) 237 final), 25 de noviembre de 2005.

Por su parte, EUROJUST se crea en 2002[2945]. En términos generales, son objetivos de esta unidad la cooperación y coordinación entre las autoridades competentes de los Estados miembro en materia de investigación y actuación judicial en relación a delitos graves que afectan a más de un Estado miembro. Cuando sea necesario para el cumplimiento de dichos objetivos, los estados miembros y Eurojust podrán intercambiar la información necesaria, y esta unidad podrá crear al efecto ficheros propios. El tratamiento de los datos en este ámbito se deberá realizar en todo caso ajustándose a lo que dispone el Convenio de 1981. En relación a los datos de salud, expresamente se señala en la normativa reguladora de Eurojust la posibilidad de manipular este tipo de información cuando se considere necesario para llevar a cabo las investigaciones pertinentes.

Europol se crea en 1995[2946] con el objetivo de mejorar la cooperación y coordinación entre las policías nacionales para luchar contra las formas graves de delincuencia. Entre sus funciones está la de recoger, compilar y analizar informaciones y datos y facilitar el intercambio de información entre estados. Para ello se creará un sistema de información propio que se surtirá de información derivada, principalmente, de sistemas de información nacionales, pero que llevará también a la creación de ficheros propios. La manipulación de la información se realizará en base a lo que dispone el Convenio de 1981 de tanta cita[2947]. La manipulación de datos de salud sólo será posible en casos excepcionales.

Además de estos instrumentos, se han suscrito otros documentos que afectan a países miembros de la UE, con la finalidad de controlar el flujo de personas y luchar contra el terrorismo. Es el caso del Tratado entre el reino de Bélgica, la República Federal de Alemania, el reino de España, la República Francesa, el Gran Ducado de Luxemburgo, el Reino de los Países Bajos y la República de Austria relativo a la profundización de la Cooperación Transfronteriza, en particular en materia de lucha contra el Terrorismo, la Delincuencia Transfronteriza y la Migración Ilegal[2948], a través del que se pretender reforzar la cooperación transfronteriza en el campo, particularmente, del intercambio de información. En este caso, la manipulación de la información plantea un problema específico pues permite el tratamiento de perfiles de ADN. También en este caso el empleo de los datos deberá realizarse conforme a los parámetros marcados por el Convenio de 1981 sobre protección de datos.

[2945] Decisión del Consejo 2002/187/JAI, 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO nº L 63/1, 6 de marzo de 2002. Modificado por Decisión del Consejo 2003/659/JAI, 18 de junio de 2003, por la que se modifica la Decisión 2002/187/JAI, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO nº L-245/44, 29 de septiembre de 2003, y por la Decisión del Consejo 2009/426/JAI, 16 de diciembre de 2008, por la que se refuerza y se modifica la Decisión 2002/187/JAI por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO nº 138/14, 4 de junio de 2009.

[2946] Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995.

[2947] ACED FÉLEZ, "La protección de datos…", cit., 2010, pp.1.367 y siguientes.

[2948] Instrumeto de ratificación de España del Convenio relativo a la profundización de la Cooperación Transfronteriza, en particular en materia de lucha contra el Terrorismo, la Delincuencia Transfronteriza y la Migración Ilegal, hecho en Prüm, 27 de mayo de 2005, BOE nº 307, 25 de diciembre de 2006. DIETRICH PLAZA, "El Tratado de Prüm…", cit., 2007.

Otro ejemplo lo constituye la creación del Sistema de Información de Visados, que contempla como instrumento la manipulación de datos y su inclusión en una base de datos centralizada. Este sistema viene a reforzar la estructura del Sistema de Información de Schengen, con el fin de controlar el flujo de las personas y tiene como finalidades facilitar el procedimiento de solicitud de visados, impedir que se incumplan los criterios para determinar el Estado miembro responsable del examen de la solicitud, facilitar la lucha contra el fraude, facilitar los controles en los puntos de paso de las fronteras exteriores y en el territorio de los Estados miembro, prestar asistencia de identificación de cualquier persona que no cumpla o haya dejado de cumplir las condiciones de entrada, estancia o residencia en territorio de los Estados miembro, contribuir a la prevención de amenazas contra la seguridad interior de cualquier Estado miembro[2949]. Este sistema de información cumplirá, también, fines relacionados con la seguridad[2950].

Todos estos sistemas de información crean un flujo de datos constante. Es cierto que al afectar, la mayoría de las veces, a estados miembros de la UE estos movimientos no se pueden considerar en base al RDLOPD transferencias internacionales en sentido estricto. Sin embargo, no está de más resaltar que la libertad con la que estos flujos se realizan encuentra justificación en el hecho de que todos los países cuentan con un sistema de protección de datos adecuado. La importancia, por lo tanto, de que un estado guarde un sistema de protección semejante se refleja en los citados sistemas de información.

Esto no quiere decir que las transferencias internacionales realizadas en estos ámbitos no generen riesgos. Más allá de los propios de toda trasmisión, el principal peligro que genera la creación de todas estas redes de información lo constituye, sin duda alguna, la puesta en común de todas las bases de datos y la creación consiguiente de grandiosas bases de datos con una ingente cantidad de información sobre multitud de personas. En alguna ocasión ya se ha puesto de manifiesto la posibilidad de que esta relación de bases de datos se dé[2951] y el Grupo de

[2949] Reglamento del Parlamento y del Consejo 767/2008 del Parlamento Europeo y del Consejo, 9 de julio de 2008, sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembro, DO nº L-218, 13 de agosto de 2008; Decisión de la Comisión 2009/377/CE, 5 de mayo de 2009, por la que se aprueban medidas de aplicación para el mecanismo de consulta y demás procedimientos contemplados en el artículo 16 del Reglamento (CE) nº 767/2008 del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembro. DO nº L-117 12 de mayo de 2009.

[2950] Decisión del Consejo 2008/633/JAI, 23 de junio de 2008, sobre el acceso para consultar el Sistema de Información de Visados (VIS) por las autoridades designadas de los Estados miembro y por EUROPOL, con fines de prevención, detección e investigación de delitos de terrorismo y otros delitos graves, DO nº L-218, 13 de agosto de 2008.

[2951] Comunicación de la Comisión al Consejo y al Parlamento Europeo sobre una mayor eficacia, interoperabilidad y sinergia ente las bases de datos europeas en el ámbito de la Justicia y los Asuntos de interior, 24 de noviembre de 2005: se trata de relacionar o interconectar los sistemas de información SIS II (que permite crear un espacio sin controles en las fronteras interiores), VIS (que mejora los procedimientos de expedición de visados) y el EURODAC (que constituye una herramienta indispensable para la eficacia del sistema europeo de asilo). Se pretende que la finalidad de la lucha contra el terrorismo justifique la puesta en común de las bases de datos y el acceso a éstas de las autoridades policiales. Se exige que esta previsión respete el derecho a la protección de datos en base al principio de proporcionalidad.

Trabajo del artículo 29 ya ha subrayado en algún momento el riesgo que ello entraña de que los ciudadanos sean objeto de un control excesivo[2952].

III.4.2. Transferencia a un país que no presenta un nivel adecuado de protección.

Fuera del entorno configurado por los países arriba citados hay un espacio en el que no se garantiza que el sistema de protección de los datos de carácter personal sea el adecuado o equiparable al reconocido en el ámbito interno. Las transferencias a estos países se erigen en operaciones con un altísimo riesgo potencial. Es por ello por lo que se entiende que resulta necesario un sistema de control de dichas operaciones para asegurarse de que los movimientos de información a estos estados se realizan con las garantías adecuadas. El punto principal de análisis de este tipo de transferencias lo constituye, por lo tanto, la construcción de dicho sistema de control.

Señala el ordenamiento que para realizar una transferencia a un país que no presenta un nivel de protección adecuado es necesaria una previa autorización del Director de la Agencia. Se establece por lo tanto un sistema de control administrativo, sujeto a un procedimiento, que finalizará con la pertinente resolución otorgando o no la autorización a la transferencia que se pretende. El RDLOPD reconoce un procedimiento determinado para otorgar estas autorizaciones[2953]. Se plantea la duda sobre el margen de actuación con el que cuenta el Director de la AEPD a la hora de permitir o no la operación. Señala la norma que este órgano "podrá otorgar" la autorización[2954]. El empleo de dichos términos parece dejar cierto margen de maniobra al Director. Sin embargo, cabe subrayar que la facultad de otorgar la autorización no constituye una potestad completamente discrecional. En primer lugar, porque los criterios para otorgar la autorización se encuentran bien definidos en el ordenamiento, por lo que una vez se cumplan dichos requisitos la Agencia deberá dar una respuesta positiva. El margen de maniobra de la Administración puede entrar en juego a la hora de valorar si se respetan o no los criterios que se van a citar a continuación, pero no más allá de estas circunstancias[2955]. En esta línea interpretativa, la Instrucción de la AEPD que regula el movimiento internacional de datos emplea los términos "será otorgada", expresión que deja menor espacio a la discrecionalidad[2956]. En segundo lugar, viene a apoyar esta idea el hecho de que el RDLOPD establezca expresamente una serie de supuestos tasados en los que se puede denegar la autorización. Esta regulación hace indicar, que fuera de estos casos el Director de la Agencia deberá otorgarla[2957].

[2952] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2005, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembro, 23 de junio de 2005.
[2953] Artículos 137 a 140 RDLOPD.
[2954] Artículo 70.2 RDLOPD.
[2955] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 592.
[2956] Norma quinta Instrucción 1/2000 de la Agencia de Protección de Datos, 1 de diciembre del 2000, relativa a las Normas por las que se rigen los Movimientos Internacionales de Datos.
[2957] Artículo 70.3 RDLOPD: "*En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1.f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes: a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el*

La autorización, según disponen las normas, se dará una vez se haya constatado que existen "garantías adecuadas" para proteger el derecho a la autodeterminación informativa de los afectados[2958]. La LOPD se refiere en términos genéricos al concepto de "garantías adecuadas", sin mencionar fórmula alguna a emplear a la hora de demostrar que éstas realmente existen. Como se ha dicho en el apartado anterior, de la LOPD podría deducirse que los requisitos para otorgar dicha autorización son los que se establecen en el artículo 33.2 de la Ley: naturaleza de los datos, finalidad y duración del tratamiento, país de origen y el país de destino, normas de derecho (generales y sectoriales) y normas de autorregulación del país de destino. En algún caso así lo llegó a considerar la doctrina, antes de que el RDLOPD fuera aprobado[2959]. Hoy día, el reglamento no deja lugar a dudas al entender que los requisitos del apartado citado no se aplican a este tipo de transferencias, sino para determinar si un país contiene un nivel adecuado de protección, a efectos de que la transmisión de datos pueda realizarse sin autorización del Director de la AEPD[2960]. En todo caso, atendiendo al contenido de los criterios que se especifican en dicha disposición, es evidente que deberán ser tenidos en cuenta en la práctica, a pesar de que no lo especifique así la Ley, a la hora de dar la autorización por el citado órgano de la Agencia.

Ante el silencio de la LOPD cabe acudir a las otras normas de referencia para determinar cómo se pueden asegurar las garantías adecuadas que permitan autorizar una transferencia internacional a un país que no guarda un nivel de protección equiparable al estatal. Disponen las normas que la carencia de un país que no presenta un nivel equiparable de protección puede suplirse, en primer lugar, a través de un contrato entre el emisor de los datos y el receptor, que asegure que se van a cumplir las garantías adecuadas de protección de dichos datos. Si esas garantías se dan, el Director de la AEPD autorizará la operación. La Directiva europea se refiere en concreto a las cláusulas contractuales, como forma o método de homologar el sistema de protección de los datos en los países que no cuentan con un sistema preestablecido suficiente[2961]. A falta de un sistema de protección de datos general en el país de destino, el importador y el exportador formalizarían un contrato en el que se obligarían a cumplir unos principios que aseguran que la manipulación de datos se llevará a cabo en un entorno seguro. El RDLOPD entra a desarrollar lo establecido por la norma europea. Dispone el reglamento que la

ejercicio por los afectados de los derechos que el contrato garantiza; b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo; c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador; d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos; e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados".

[2958] Artículo 33.1 LOPD; Artículo 70.1 RDOLPD: "*Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos*".

[2959] COUDERT, "Transferencias Internacionales…", cit., 2007, p. 443.

[2960] Artículo 67.1 RDLOPD.

[2961] Artículo 26.2 Directiva 95/46/CE: "*Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas*".

autorización se otorgará cuando el responsable exportador presente un contrato escrito acordado entre él y el importador, que garantice de manera suficiente la protección de los derechos y libertades de las personas afectadas por la transferencia, fundamentalmente del derecho a la vida privada[2962].

En la práctica, y si se atiende a las autorizaciones que hasta ahora ha emitido la Agencia, en la gran mayoría de transferencias el cumplimiento de las garantías adecuadas se justifica mediante este tipo de contratos. En estos casos lo primordial será determinar el contenido que deberán guardar dichas cláusulas. Para ello, el reglamento, en vez de concretar por sí mismo, tal como lo hacía la Instrucción de la AEPD reguladora de los movimientos internacionales de datos[2963], dicho contenido, realiza una remisión a diferentes decisiones de la Comisión Europea que establecen un contenido tipo de los distintos contratos que se pueden formalizar[2964]. No se cree necesario realizar un análisis exhaustivo sobre las características que han de guardar las cláusulas contractuales indicadas[2965]. En términos generales, las obligaciones impuestas al exportador e importador de datos en las citadas decisiones configuran un sistema suficientemente riguroso. El primero está obligado, entre otras cosas, a verificar si el importador de los datos es capaz de cumplir las cláusulas del contrato, a facilitar una copia del contrato al afectado, cuando éste lo pida, o a colaborar con la Agencia de Protección de Datos[2966]. El segundo tiene la obligación, fundamentalmente, de asegurar que la legislación de su país que le es aplicable no le impide cumplir con las obligaciones del contrato, de colaborar con el exportador de datos y con la autoridad de control correspondiente para demostrar que cumple con las garantías necesarias[2967]. Como bien ha señalado el Grupo de Trabajo del artículo 29, será necesario que el contrato recoja los principios básicos de protección de datos que se reconocen

[2962] Artículo 70.2 RDLOPD: "*La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.*
A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE".

[2963] Norma quinta Instrucción 1/2000 de la AEPD, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos.

[2964] Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001, relativa a Cláusulas Contractuales Tipo para la Transferencia de Datos Personales a un Tercer País previstas en la Directiva 95/46/CE, en DO nº L-181/19, 4 de julio de 2001; Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004 por la que se modifica la Decisión 2001/497/CE en lo relativo a la Introducción de un Conjunto Alternativo de Cláusulas Contractuales Tipo para la Transferencia de Datos Personales a Terceros Países, en DO nº L-385/74 de 29 de diciembre de 2004; Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, DO nº L-6/52, 10 de enero de 2002. A éstas hay que añadir la recientemente aprobada Decisión 2010/87/UE de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, DO nº L-39/5, 12 de febrero de 2010.

[2965] SANCHO VILLA, *Negocios Internacionales…*, cit., 2010, pp. 124-128 y 135 y siguientes, realiza un interesante análisis sobre la función y contenido de estos contratos.

[2966] Cláusula 4ª de la Decisión 2001/497/CE, de 15 de junio de 2001.

[2967] Cláusula 5ª, de la Decisión 2001/497/CE, de 15 de junio de 2001.

en la Directiva, y por ende en la LOPD (calidad, información, seguridad y derechos), y determine la fórmula por la que dicho contrato puede hacerse efectivo y ejecutarse[2968].

Además de las cláusulas contractuales a las que se hace referencia tanto en la Directiva europea como en el RDLOPD, esta última norma recoge otra fórmula por la que se puede demostrar que existen garantías suficientes que justifiquen la autorización del Director de la Agencia para realizar una transferencia determinada. El reglamento señala que pueden autorizase las transmisiones realizadas entre grupos multinacionales de empresas, cuando éstas hubieran adoptado reglas o normas internas que garanticen un suficiente nivel de protección[2969]. Parece que aquí la norma se está refiriendo a las antes mencionadas *Binding Corporate Rules*. En este caso, este tipo de normas o reglas no actúan como un sistema de autorregulación que ayuda a determinar el carácter adecuado de un sistema de protección determinado en un país, sino que se emplean como criterio para concluir que existen las garantías suficientes para autorizar una determinada transferencia de datos[2970]. El principal problema que plantean estas reglas es el relativo a la necesidad de probar que existen mecanismos suficientes para obligar a las entidades adscritas a dichos criterios a cumplirlos[2971]. En este sentido, el propio reglamento exige que para otorgar la autorización a la transmisión basándose en estas *Binding Corporate Rules* será necesario que el cumplimiento de estas reglas pueda ser exigible de acuerdo al ordenamiento jurídico español.

En principio, el ordenamiento recoge expresamente estas herramientas como las que se pueden emplear para asegurar que se cumplen las garantías adecuadas. Se plantea por la doctrina la posibilidad de que, más allá de los contratos y las fórmulas de las reglas corporativas, la AEPD pueda basar la autorización en otros criterios que lleven a la conclusión de que existen garantías suficientes[2972]. Esta consideración podría tener sentido haciendo la siguiente interpretación: el hecho de que un país no haya sido considerado como portador de un sistema "adecuado" de protección de datos por la Comisión o la autoridad competente de algún país no significa que no confiera una garantía suficiente. Puede que, simplemente, su sistema de protección no haya sido analizado. En este sentido, a pesar de no contar oficialmente con un nivel de protección adecuado, puede ocurrir que la AEPD autorice una transferencia concreta a

[2968] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre la transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE, 24 de julio de 1998.

[2969] Artículo 70.4 RDLOPD: "*También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.*
En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.
En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento".

[2970] FERNÁNDEZ-LONGORIA y FERNÁNDEZ-SAMANIEGO, "Transferencias internacionales…", cit., 2010, p. 1.789.

[2971] ÁLVAREZ RIGAUDIAS, "Las transferencias internacionales…", cit., 2010, p. 1.809.

[2972] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 623.

dicho país, aunque no haya contrato, si se demuestra que de facto sí hay protección suficiente. Parece que esta consideración la podría hacer la AEPD aplicando los criterios arriba descritos, que se emplean para determinar sí un país cuenta con un nivel de protección adecuado. En todo caso, si esta Agencia encuentra argumentos suficientes para justificar la transferencia a dicho país por considerar que mantiene un nivel de protección adecuado, deberá iniciar el procedimiento para emitir la resolución por la que se fije dicho país dentro de la lista de países por los que los datos pueden fluir sin necesidad de autorización alguna.

Más allá de estos supuestos no se imagina otra fórmula alternativa al contrato o a las citadas reglas corporativas, con las que se pueda garantizar el cumplimiento de los principios de protección de datos. Se entiende aquí que, fuera de estos casos, si se admitiera una facultad mayor al Director de la AEPD para autorizar las transferencias internacionales, se le estaría atribuyendo un margen de discreción excesivo. Las herramientas que se han reconocido hasta ahora tienen su encaje de una manera o de otra en el ordenamiento. Más allá de los casos expuestos, las autorizaciones que pudiera otorgar el Director no encontrarían base jurídica en el ordenamiento y se ajustarían a criterios propios, subjetivos, fuera de los establecidos en las normas.

Como ocurriera en el apartado anterior, puede suceder que las circunstancias que rodean a una transferencia determinada sean valoradas de forma diferente en estados distintos y que los criterios que guíen las autorizaciones acaben siendo completamente divergentes en los estados miembros. Para evitar contradicciones sustanciales en este sentido dispone la Directiva que las autorizaciones que se emitan en cumplimiento de lo dispuesto en las líneas anteriores deberán comunicarse a los demás Estados miembros de la UE y a la propia Comisión Europea para que puedan mostrar, en su caso, los argumentos por los que se oponen a la emisión de alguna autorización[2973].

Todas las herramientas que se han expuesto suponen la incorporación de nuevas fórmulas que permiten a los diferentes actores llevar a cabo una transferencia internacional garantizando un adecuado nivel de protección. Se trata de simplificar y facilitar los procesos de transferencia[2974]. Evidentemente, esta circunstancia favorece la circulación de los datos, lo cual, desde el punto de vista sobre todo económico, puede valorarse de manera positiva, pues hace posible que se lleven a cabo operaciones que de lo contrario no podrían realizarse. Este hecho, sin embargo, no puede esconder los recelos que desde el punto de vista de la protección de los datos de carácter personal estas fórmulas provocan. El recelo resulta del hecho de que los

[2973] Artículo 26 Directiva 95/46/CE: "*3. Los Estados miembros informarán a la Comisión y a los demás Estados miembros acerca de las autorizaciones que concedan con arreglo al apartado 2.*
En el supuesto de que otro Estado miembro o la Comisión expresaran su oposición y la justificaran debidamente por motivos derivados de la protección de la vida privada y de los derechos y libertades fundamentales de las personas, la Comisión adoptará las medidas adecuadas con arreglo al procedimiento establecido en el apartado 2 del artículo 31.
Los Estados miembro adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión.
4. Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembro adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".

[2974] Memoria AEPD 2008. Se pone de manifiesto el esfuerzo que se está realizando, fundamentalmente por el Grupo de Trabajo del artículo 29, por flexibilizar los flujos de información, principalmente ente empresas de grandes corporaciones multinacionales.

instrumentos planteados, contratos y reglas corporativas, constituyen un objeto cuyo cumplimiento puede resultar difícil de controlar[2975]. Es cierto que a la hora de autorizar las transferencias en base a dichos instrumentos el contenido de éstos podrá ser fiscalizado por la Agencia, determinando que existen las garantías suficientes. No obstante, una vez se haya efectuado la transmisión de la información dicho control en el país importador resulta más complejo al tratarse de un país cuyo ordenamiento no garantiza un nivel adecuado de protección. Es por ello que se subraya aquí la necesidad de que se establezcan todas las medidas posibles para que el cumplimiento de los contratos y las reglas de las *Binding Corporate Rules* sea efectivo y para que el titular de los datos que se manipulan tenga conocimiento de las herramientas de las que dispone en caso de que tenga que exigir responsabilidades.

III.4.3. El *outsourcing* internacional.

En un principio, cuando se habla de la transferencia internacional de datos se piensa en la transmisión de datos entre dos sujetos responsables de ficheros. El exportador realiza la transferencia a un importador que manipulará la información para cumplir sus propios fines. En este sentido, esta operación podría ser equiparable a la cesión de datos. Sin embargo, no es de extrañar encontrarse en la realidad con el supuesto en que la transferencia internacional se realiza no a otro sujeto responsable, sino a una empresa contratada para manipular los datos en nombre del exportador responsable. De hecho, hace ya unos años que se puso de manifiesto que este tipo de operaciones constituía la principal modalidad de transferencia[2976]. Hoy día no hay más que atender a las autorizaciones otorgadas por la AEPD para darse cuenta que, efectivamente, este tipo de transmisiones son las que mayor aplicación tienen en la realidad. En estos casos un responsable situado en territorio estatal emplea medios situados fuera de sus fronteras para cumplir sus finalidades en el Estado. El importador no sería otra cosa que un encargado del tratamiento que accedería a los datos por cuenta del responsable exportador.

Ni la Directiva, ni la LOPD, ni el reglamento que la desarrolla hacen mención expresa a esta figura. En el caso de esta última norma, en el apartado dedicado a las cláusulas contractuales que se han de formalizar para obtener la autorización del Director, simplemente se hace referencia a la Decisión de la Comisión que determina las cláusulas que deberá contener el contrato a formalizar entre el responsable exportador y el encargado importador para que la transferencia se pueda autorizar, Decisión que ha sido recientemente derogada[2977]. Sí se refiere a la figura que ahora se analiza la Instrucción de la AEPD que regula las transferencias internacionales, que destina un apartado completo a esta figura[2978]. Este apartado, que en parte

[2975] REIDENBERG, "Oportunidades y...", cit., 2006, pone de manifiesto los riesgos de este proceso de simplificación de las vías para garantizar la protección de datos en las transferencias internacionales.
[2976] Memoria de la AEPD 2006.
[2977] SANCHO VILLA, *Negocios Internacionales*..., cit., 2010, p. 156 y siguientes, realiza un exhaustivo análisis del contenido de la nueva Decisión de la Comisión.
[2978] Norma sexta Instrucción 1/2000 de la AEPD, 1 de diciembre del 2000 relativa a las normas por las que se rigen los movimientos internacionales de datos: "*1. Cuando la transferencia internacional de datos tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, la realización del tratamiento deberá estar regulada en un contrato, en que deberá hacerse constar la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario.*
El contrato, que deberá constar por escrito, establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en

fue anulado por los tribunales[2979], simplemente traslada lo dictado por la Ley en relación al acceso por cuenta de terceros a este ámbito, haciendo especial hincapié en la necesidad de redactar un contrato entre responsable y encargado con todas las garantías. Es de subrayar que en este caso se señala expresamente que el contrato deberá quedar formulado de forma escrita.

En este tipo de operaciones el encargado importador puede situarse tanto en un país que cuenta con un nivel adecuado de protección como en un Estado que no guarda un sistema equiparable de protección de datos. En el primer caso la transmisión se someterá a las reglas de control comunes para estos casos, que se verán en el apartado siguiente. No hay que olvidar, que en el ámbito interno la LOPD exige que el acceso a los datos por cuenta de terceros ha de regularse, ya sea en el ámbito interno o internacional, a través de un contrato entre el responsable y el encargado[2980]. En el segundo supuesto, el acceso por cuenta de terceros deberá someterse al control previo de la autorización, autorización que se dará si se cumplen las garantías adecuadas. Ya se ha visto que la principal fórmula por la que se demuestra que estas garantías se guardan es la forma contractual. Se debe formalizar un contrato entre el responsable y el encargado que se sitúa en un país extranjero para asegurar que la transferencia se realizará en un entorno seguro. Este contrato se sumará al rutinario contrato que ha de formalizarse en todo caso en que se produce un acceso por cuenta de tercero.

En principio parece obvio que han de aplicarse aquí las reglas que en los apartados anteriores se han descrito para las transmisiones entre responsables de ficheros. Sin embargo la citada Instrucción plantea alguna duda al respecto. En esta norma el apartado relativo al *outsourcing* internacional se aplica indistintamente tanto a los supuestos de transferencias realizadas a países que presentan una protección equiparable a la del Estado español como a los casos en que esa protección no existe. En el primer caso, siguiendo la regla general establecida para este tipo de accesos, no habría que solicitar la autorización del Director de la AEPD. Para el segundo caso, la Instrucción tampoco exige expresamente el requisito de la autorización del Director. Podría pensarse que esta situación lleva a la conclusión de que el

dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español.
Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento
2. La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.
En consecuencia, si la transmitente deseara que por parte de varias entidades distintas, situadas fuera del territorio español, se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la Ley Orgánica 15/1999, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.
3. En caso de que la transferencia se dirija a un destinatario situado en un Estado no miembro de la Unión Europea respecto del que no se haya declarado la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, en el contrato deberán constar cautelas semejantes a las indicadas en la norma quinta en lo referente al régimen sancionador y de indemnización a los interesados, así como en lo relativo a las potestades de la Agencia de Protección de Datos, para el caso en que la destinataria emplee los datos para otra finalidad distinta de la que motivó la transferencia, los comunique o los utilice incumpliendo las estipulaciones del contrato".

[2979] SAN 15 de marzo de 2002, FFJJ 11 y 12.
[2980] Artículo 12 LOPD.

acceso por cuenta de terceros realizado por un importador situado en un país que no cuenta con un nivel de protección adecuado no requiere de autorización previa del Director de la Agencia.

Se entiende aquí, que de la misma manera que los contratos que posibilitan la transferencia internacional entre responsables de ficheros son sometidos a una previa autorización de dicho órgano, lo mismo ha de ocurrir con los contratos que abren la puerta al *outsourcing* internacional. A pesar de tratarse de un acceso por cuenta de terceros no deja de ser una transmisión a un Estado que no presenta las garantías adecuadas para la protección de los datos de carácter personal. Así, será necesario que el órgano competente determine si el contrato garantiza que la transmisión vaya a realizarse con las garantías suficientes.

Hoy día, el nuevo reglamento aclara las dudas que podían generarse al respecto. La referencia a la Decisión de la Comisión Europea que regula el acceso por cuenta de terceros con alcance internacional se incardina en el apartado dedicado a las transferencias que requieren de la autorización del Director. De esta manera no cabe duda alguna de que este tipo de operación deberá realizarse, cuando la transmisión se haga a un país que no presenta un nivel adecuado de protección, sometiéndose a la autorización del citado órgano. Así se aclara también en los informes jurídicos de esta institución que se refieren a esta cuestión. En dichos textos se apunta la necesidad de aplicar tanto la regulación referida al acceso a datos por cuenta de terceros como las garantías pertinentes que deben adoptarse, por tratarse de una transferencia internacional, a efectos de que se otorgue la autorización[2981].

Estas garantías pasan porque se formalice un contrato o acuerdo que asegure que en el país importador la manipulación de los datos se realizará en un entorno seguro. El Reglamento hoy vigente hace mención expresa a una Decisión de la Comisión Europea, que precisamente se dirige a determinar qué cláusulas contractuales ha de incluir un contrato entre un responsable exportador y un encargado importador para que la transmisión de datos pueda realizarse.[2982]. Se entiende que los contratos que integren las exigencias de la citada Decisión podrán ser objeto de autorización. Como se ha dicho más arriba, la norma europea citada por el RDLOPD ha sido derogada con la entrada en vigor en 2010 de una nueva Decisión de la Comisión, que actualiza los requisitos exigidos por la Decisión derogada y regula aspectos que ésta última no recogía, caso de la figura del sub-encargado[2983].

El contenido de las cláusulas contractuales tipo referidas a este tipo de operaciones se asemeja al que se ha descrito al analizar los contratos realizados en las transferencias internacionales en las que se implican dos responsables. En este sentido las obligaciones impuestas al exportador y al importador se dirigen a que se garantice que la manipulación en el país de destino respete los principios de protección de datos recogidos en la Directiva europea y

[2981] Informe jurídico 0391/2007, de la AEPD.
[2982] Decisión 2002/16/CE de la Comisión, de 27 de diciembre de 2001, relativa a Cláusulas Contractuales Tipo para la Transferencia de Datos Personales a los Encargados del Tratamiento establecidos en Terceros Países, de conformidad con la Directiva 95/46/CE..
[2983] Decisión 2010/87/UE de la Comisión de 5 de febrero de 2010 relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, DO nº L-39/5, 12 de febrero de 2010.

a que se establezcan mecanismos para que los interesados puedan exigir el cumplimiento por parte del encargado del tratamiento importador de dichos principios y, en su caso, responsabilidades. En todo caso, tanto la anterior Decisión de la Comisión como la actual hacen hincapié en dos puntos. En primer lugar, en la necesidad de que el encargado se limite, en todo caso, a cumplir las instrucciones establecidas en el contrato por el responsable exportador. El exportador está obligado a determinar las instrucciones, fijar las medidas técnicas y organizativas que el importador deberá adoptar para que el tratamiento se realice en un entorno seguro y asegurarse de que el importador adopta dichas medidas. El importador está obligado a respetar dichas instrucciones, asegurarse de que la normativa del país donde va a manipular los datos no es obstáculo para cumplir dichas instrucciones y cumplir con las medidas de seguridad establecidas en el contrato. En segundo lugar, se subraya la necesidad de que el interesado cuente con mecanismos para exigir responsabilidades en caso de que se cometa alguna infracción. Evidentemente, no se puede considerar que se dan las garantías adecuadas para autorizar un acceso por cuenta de tercero de alcance internacional si no se establecen instrumentos para que el afectado pueda exigir responsabilidades al exportador o al importador.

La principal novedad que incorpora la nueva Decisión de la Comisión es la inclusión de la figura del sub-encargado[2984]. Como señalaba el dictamen del Grupo de Trabajo del artículo 29 de la Directiva en relación al proyecto de dicha Decisión, la realidad exigía que se regulara la figura del sub-encargado, cosa que no hacía la hoy derogada Decisión[2985]. Al igual que en el ámbito interno, también en el internacional es cada vez más común que los propios encargados del tratamiento de datos subcontraten otra empresa para que gestione parte de los servicios que presta e incluso que estos sub-encargados contraten a su vez a otra empresa con el mismo fin[2986]. Como se ve, es posible de esta forma crear auténticas cadenas en las que los datos son manipulados en diferentes lugares del planeta. No se va a realizar en este momento un análisis exhaustivo sobre la problemática que plantea esta figura, pues supera los fines que se persiguen en este trabajo, pero merece la pena realizar un breve apunte al respecto.

La derogada Decisión no entraba a regular esta figura y la indeterminación sobre si era posible o no y, en caso de que sí lo fuera, cómo llevar a cabo la subcontratación era grande. Así se ponía de manifiesto por la AEPD en alguna de sus memorias[2987]. De inicio, tal y como se reconocía en algún informe jurídico de la Agencia, la normativa parecía rechazar la posibilidad de llevar a cabo la subcontratación[2988]. La Decisión de la Comisión de 2002 se refería en todo caso a la relación entre el responsable del fichero y el encargado, por lo que no parece que tuviera cabida la relación entre dos encargados. No obstante, en última instancia, consciente de la necesidad real de que este tipo de operaciones se puedan dar, el informe jurídico reconocía la viabilidad de la subcontratación siempre y cuando se asegurara que el encargado que exporta los

[2984] SANCHO VILLA, *Negocios Internacionales…*, cit., 2010, p. 158.
[2985] Dictamen 3/2009 del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el proyecto de Decisión de la Comisión relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE, 5 de marzo de 2009.
[2986] FERNÁNDEZ-LONGORIA y FERNÁNDEZ-SAMANIEGO, "Transferencias internacionales…", cit., 2010, p. 1.796.
[2987] Memoria de la AEPD 2007.
[2988] Informe jurídico 0108/2008 de la AEPD.

datos al sub-encargado actuaba en nombre del responsable y que este sub-encargado aceptaba el cumplimiento de las garantías adecuadas de protección de datos. La Decisión de 2010 entra a regular la figura de la subcontratación para que la indeterminación de las normas no se convierta en un limbo jurídico en el que estas operaciones se puedan realizar sin mayor control. Esta Decisión dispone una serie de exigencias que obligan a que la subcontratación se realice con todas las garantías. Evidentemente, la subcontratación sólo podrá realizarse en el ámbito de los servicios contratados inicialmente ente el responsable y el primer encargado. En general, las garantías se resumen en la necesidad de que en el contrato entre el encargado y el sub-encargado el último se sujete a las mismas obligaciones que el primero y a la necesidad de que el responsable consienta la operación.

La Decisión en ningún momento hace referencia a la necesidad de que las autoridades de control de los estados deban autorizar estas operaciones. Simplemente establece un sistema de control a posteriori, bien habilitando a las citadas autoridades de control a realizar inspecciones o bien posibilitando que el afectado exija responsabilidades en caso de que haya un incumplimiento de la normativa de protección de datos. Se defiende aquí que estas operaciones requieren de la autorización del Director de la AEPD. Como bien señala el Grupo de Trabajo de tanta cita, la posibilidad que abre la Decisión puede llevar a crear extensas redes o flujos de información entre subcontratistas cuya actividad puede ser difícil de fiscalizar, sobre todo a la hora de pedir responsabilidades. La necesidad de controlar todas estas operaciones pasa por exigir la autorización del órgano administrativo. Esta exigencia puede encontrar apoyo en la normativa. Por un lado, en la medida en que el RDLOPD exige la autorización del Director para habilitar un tratamiento de datos por parte de un encargado en un país que no garantiza un nivel adecuado de protección, no hay razón para que no se aplique la misma medida cuando la transmisión se va a realizar entre dos encargados. Por otro lado, la Decisión de 2010 dispone que las cláusulas que regulan esta decisión aseguran que se cumplen las garantías adecuadas. Como señala la LOPD las garantías adecuadas establecen la condición necesaria para otorgar la autorización. Es necesario que este órgano verifique que se cumplen dichas garantías. Por último, se establece en esta norma la obligación del exportador de asegurarse de que el contrato entre el encargado y subcontratado respeta las mismas garantías que en el contrato entre el responsable y el encargado. Entre esas garantías, se entiende aquí, ha de incardinarse la necesidad de que el Director de la AEPD autorice las transferencias realizadas a países que no guardan un nivel de protección adecuado.

III.4.4. Supuestos en que el régimen general de protección de datos en las transferencias internacionales queda exceptuado.

Como se ha visto hasta ahora, el régimen general expuesto en los apartados precedentes viene a asegurar que las transferencias se lleven a cabo en todo caso con unas mínimas garantías de que el derecho a la autodeterminación informativa va a resultar salvaguardado. Frente a este régimen general establecido en el artículo 33, la LOPD, siguiendo lo dictado por la Directiva europea[2989], recoge una serie de casos en que no se aplica la regulación que se ha

[2989] Artículo 26.1 Directiva 95/46/CE: "*No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembro dispondrán que pueda efectuarse una*

comentado hasta ahora. Según dispone la Ley, en los supuestos reconocidos en el artículo 34 las transferencias podrán llevarse a cabo, tanto a países que cuentan con un nivel de protección adecuado como a los que no, sin necesidad de someterse al control administrativo dispuesto en el régimen general regulador de estas operaciones, fundamentalmente a la autorización. Una regulación similar se recoge en el Protocolo Adicional al Convenio del Consejo de Europa de protección de datos[2990]. Se trata, por lo tanto, de unos supuestos en que las transmisiones de datos se realizan, en un inicio, con gran libertad y sin garantías especialmente rigurosas. Piénsese que se está abriendo la puerta a la posibilidad de remitir información, de cualquier naturaleza, a cualquier punto del planeta, sin necesidad de someterse a los criterios de control establecidos generalmente para las transferencias. Evidentemente, la situación de minoración de las garantías requiere de justificación. Esta justificación vendrá de la relevancia de las finalidades que persiguen las transferencias recogidas en este grupo. Lo importante en estas operaciones no es, como lo era hasta ahora, el nivel de protección que se otorga a los datos de carácter personal en el país importador, sino la relevancia del objetivo que se pretende conseguir con el movimiento de la información.

El contenido del artículo 34 se ha trascrito más arriba. La LOPD amplía, siguiendo lo establecido por la Directiva, la lista de supuestos exceptuados que recogía la anterior Ley orgánica de protección de datos[2991]. Las excepciones son muy variadas y responden a motivos

transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
a) el interesado haya dado su consentimiento inequívocamente a la transferencia previa, o
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta".

[2990] Artículo 2 Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001: "*Flujos transfronterizos de datos de carácter personal hacia un destinatario que no está sujeto a la jurisdicción de una Parte en el Convenio. 1. Cada Parte dispondrá que la transferencia de datos de carácter personal hacia un destinatario sometido a la jurisdicción de un Estado u organización que no sea Parte en el Convenio sólo podrá efectuarse si dicho Estado u organización garantiza un nivel de protección adecuado a la transferencia de datos prevista.*
2. No obstante lo dispuesto en el apartado 1 del artículo 2 del presente Protocolo, cada Parte podrá permitir la transferencia de datos de carácter personal: a) si está prevista en su legislación interna a causa de: intereses específicos de la persona interesada, o de intereses legítimos prevalecientes, en particular, intereses públicos importantes, o; b) si la persona responsable de la transferencia ofrece garantías, que, en particular, pueden resultar de cláusulas contractuales, y éstas son juzgadas suficientes por la autoridad competente de conformidad con el derecho interno".

[2991] Artículo 33 LORTAD: "*Lo dispuesto en el artículo anterior no será de aplicación:*
a. Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de Tratados o Convenios en los que sea parte España.
b. Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c. Cuando la misma tenga por objeto el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica o brotes epidémicos.

diferentes. Indudablemente, llama la atención que por un lado se haga especial hincapié en que las transferencias hayan de realizarse con todas las garantías posibles y por otro se establezcan supuestos exceptuados que si son interpretados en un sentido amplio podrían llegar a vaciar de contenido los principios generales que han de guiar las transferencias internacionales[2992]. El reglamento que desarrolla la Ley estatal no concreta el contenido de las excepciones, simplemente realiza una remisión a la letra de la LOPD. Antes de la entrada en vigor de este reglamento, el anterior que desarrollaba la LORTAD matizaba el contenido de dicha Ley. Es más, dicha disposición general recogía nuevos supuestos, no previstos en la Ley, en los que el régimen jurídico general quedaba exceptuado. Evidentemente, es cuestionable que una norma de rango reglamentario entre a establecer, *ab initio*, los supuestos en que las transferencias internacionales pueden realizarse sin atender al régimen general. No obstante, cierto es que la letra de dicha norma hacía referencia a supuestos en que parece justificada, haciendo una interpretación sistemática del ordenamiento, la excepción a la autorización, pues responden a motivos de interés general como investigaciones policiales o de materia tributaria[2993]. En todo caso, y si bien es cierto que estas excepciones no aparecen recogidas de manera expresa en el ordenamiento estatal hoy día vigente, lo cierto es que tienen plena aplicación pues responden a motivos recogidos en acuerdos internacionales como el de Schengen, que crean flujos de información que afectan directamente a los datos de los ciudadanos del Estado.

No interesa en este momento realizar una descripción detallada sobre cada uno de los supuestos en que la autorización se exceptúa. No obstante, no puede dejar de llamarse la atención sobre las referencias que se hacen a la posibilidad de aplicar la excepción en los casos en que la transferencia sea precisa para la ejecución de un contrato o precontrato y la referencia a la posibilidad de justificar la excepción por consentimiento del titular de los datos.

Se dice aquí que llaman la atención estos supuestos debido a que, tanto en un caso como en el otro, dejar al albur de la autonomía de los intervinientes la posibilidad de transmitir datos de

d. Cuando se refiera a transferencias dinerarias conforme a su legislación específica".

[2992] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 595; SANCHO VILLA, *Negocios Internacionales…*, cit., 2010, p. 125.

[2993] Artículo 4.1 RD 1332/1994, 20 de junio de 2004, por el que se Desarrollan Algunos Puntos de la LORTAD: "*exceptúan, en todo caso de la autorización previa del Director de la Agencia de Protección de Datos las transferencias de datos de carácter personal que resulten de la aplicación de tratados o convenios en los que sea parte España y, en particular:a) Las transmisiones de datos registrados en ficheros creados por las Fueras y Cuerpos de Seguridad en función de una investigación concreta, hechas por conducto de INTERPOL u otras vías previstas en convenios en los que España sea parte, cuando las necesidades de la investigación en curso exijan la transmisión a servicios policiales de otros Estados.*

b) Las transmisiones de datos registrados en la parte nacional española del Sistema de Información Schengen, con destino a la unidad de apoyo del sistema, a los solos efectos de una investigación policial en curso que requiera la utilización de datos del sistema.

c) Las transmisiones de datos previstas en el sistema de intercambios de información contemplado en el Título VI del Tratado de la Unión Europea.

d) Las Transmisiones de los datos registrados en los ficheros creados por las Administraciones tributarias, a favor de los demás Estados miembros de la Unión Europea o a favor de otros Estados terceros, en virtud de los dispuesto en los convenios internacionales de asistencia mutua en materia tributaria.

2. Se exceptúan, asimismo, de la autorización previa del Director de la Agencia de Protección de Datos, cualquiera que sea el Estado destinatario de los datos, las transmisiones de datos que se efectúen para cumplimentar exhortos, cartas, órdenes, comisiones rogatorias u otras peticiones de auxilio judicial internacional, y los demás supuestos previstos en el artículo 33 de la Ley Orgánica 5/1992".

carácter personal, independientemente del contenido de la información que se trate, a países que no cuentan con un sistema de protección adecuado es criticable[2994]. En principio, esta previsión podría parecer plenamente coherente con el contenido del derecho a la autodeterminación informativa, que no es otra cosa que la capacidad de controlar los datos que a cada uno conciernen. Sin embargo, se entiende que el hecho de que una transferencia internacional de datos quede a completa disposición de los sujetos que participan en la relación, incluso cuando se trata de datos sensibles como los sanitarios, puede resultar un tanto arriesgado. En primer lugar, debido a que en el caso de las Transferencias Internacionales es muy improbable que el afectado llegue a conocer el riesgo real que conlleva una operación de esas características, que permite la remisión de la información a un país que no guarda el nivel de protección adecuado. Y en segundo lugar, porque muchas veces la autonomía de los afectados a la hora de realizar un contrato o dar el consentimiento no es plena[2995]. Las partes que formalizan un contrato no siempre se encuentran en igualdad de condiciones.

Partiendo de las premisas que se señalan, desde instancias internacionales se ha abogado por realizar una interpretación de estas excepciones desde una perspectiva más proteccionista o garantista del derecho a la autodeterminación informativa. Hay que tener en cuenta que estas situaciones habilitan o generan un flujo de datos, de alguna manera incontrolado. Se asume cuando se aplican estas excepciones que, una vez hayan sido trasladados, los datos pueden ser empleados en los países importadores de una manera que en atención a la normativa interna podría ser considerada contraria a Derecho. Por ello, en primer lugar, ha subrayado el Grupo de Trabajo del artículo 29, en referencia a la Directiva, la necesidad de hacer una interpretación restrictiva de las excepciones[2996]. Y en segundo lugar, el mismo órgano ha señalado que la aplicación de estas excepciones será posible sólo como una *última ratio,* cuando no sea posible fijar una vía de protección adecuada atendiendo a los medios que la propia Directiva dispone en los artículos 25 y 26, y cuando la transferencia sea absolutamente necesaria. Es decir, siempre que se pueda se establecerán formas de garantizar dicha protección cuando se trate de transferir datos de carácter personal a países que no presentan una protección equiparable, independientemente de que pueda aplicarse una de las excepciones a la autorización recogidas en las normas[2997].

No hay que olvidar tampoco que la aplicación de las excepciones no libera del cumplimiento de los deberes y obligaciones que impone la LOPD para todo tratamiento. Así lo ha subrayado también la jurisprudencia[2998]. Los derechos a consentir y a ser informado, fundamentalmente,

[2994] SANCHO VILLA, *Negocios Internacionales…*, cit., 2010, pp. 129-130, analiza estos dos supuestos.
[2995] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 597. Documento de Trabajo del Grupo de Trabajo del artículo 29, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, 25 de noviembre de 2005.
[2996] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre Transferencias de Datos Personales a Terceros Países: Aplicación de los artículos 25 y 26 de la Directiva sobre Protección de Datos de la UE, de 24 de julio de 1998. Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, 25 de noviembre de 2005.
[2997] SAN 21 de julio de 2004, FJ 9. Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, 25 de noviembre de 2005.
[2998] SAN de 15 de marzo de 2002, FJ. 3.

tienen plena vigencia en estos casos. Habrá que atender a los motivos que justifican la transferencia internacional en cada caso para determinar si dichos derechos pueden verse, como la citada autorización, exceptuados.

III.5. El control de la APD sobre las transferencias internacionales.

En todos los casos de transferencia que se han visto, tanto en los que es necesaria la autorización del Director de la AEPD como en los que no, será fundamental que todas las garantías que las diferentes normas exigen se respeten con rigurosidad. Corresponde a la Agencia llevar a cabo este control, en su caso, en el momento en que se lleve a cabo la autorización, o siempre, cuando la transferencia se inscriba en el registro correspondiente. La importancia de este ejercicio de fiscalización ha sido puesta de manifiesto en el Protocolo Adicional al Convenio del Consejo de Europa sobre protección de datos[2999].

Ni la LOPD ni la Directiva europea establecen claramente hasta dónde llega la capacidad de control de la AEPD con respecto a estas operaciones, debiendo acudir al reglamento que desarrolla la Ley y a la Instrucción de la Agencia que regula los movimientos internacionales de datos, para deducir cuál es la fórmula que se sigue a la hora de comprobar que se han cumplido los requisitos necesarios para que la transferencia internacional se ajuste a las exigencias que se han apuntado.

A) En primer lugar, en relación a las transferencias realizadas a los países que presentan un nivel de protección adecuado, el control se realiza fundamentalmente en dos aspectos. Por un lado, el ordenamiento exige que toda transferencia haya de ser notificada a la Agencia a efectos de que quede registrada en el registro pertinente. El RDLOPD recoge expresamente esta obligación de notificar[3000]. Sin embargo, la redacción del reglamento podría plantear alguna confusión en relación a la necesidad de notificar las transferencias cuando éstas se realizan a países que presentan un nivel de protección adecuado. La ubicación de la exigencia de notificación en un precepto, el artículo 66, encabezado con los términos "Autorización y notificación", podría llevar a entender que la notificación sólo es exigible en las transferencias llevadas a cabo con autorización del Director de la AEPD. El precepto hace referencia a la necesidad de autorización de este órgano para realizar determinado tipo de transferencias internacionales y en el último apartado señala la obligación de notificar dicha operación. Podría interpretarse que las transferencias que no requieren de dicha autorización, por realizarse a países que cuentan con un nivel de protección adecuado, no exigen tampoco su notificación a la

[2999] Artículo 1 Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las Autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo el 8 de noviembre de 2001: "*1. Cada Parte dispondrá que una o más autoridades sean responsables de garantizar el cumplimiento de las medidas previstas por su derecho interno que hacen efectivos los principios enunciados en los Capítulos II y III del Convenio, así como en el presente Protocolo.*
2.a) A este efecto, las autoridades mencionadas dispondrán, en particular, de competencias para la investigación y la intervención, así como de la competencia para implicarse en las actuaciones judiciales o para llamar la atención de las autoridades judiciales competentes respecto de las violaciones de las disposiciones del derecho interno que dan efecto a los principios mencionados en el apartado 1 del artículo 1 del presente Protocolo".

[3000] Artículo 66 RDLOPD: "*En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento*".

Agencia. Como era de esperar, una interpretación sistemática de la Ley niega esta interpretación. La Ley obliga a que toda transferencia sea notificada en todo caso, tanto cuando se trata de ficheros públicos[3001] como privados[3002], cualquiera que sea la circunstancia en la que se dé, se haga a un país que cuente con un nivel adecuado de protección o no. Tiene sentido esta interpretación en la medida en que la obligación de notificar responde a la necesidad de controlar las operaciones que se realizan con los datos de carácter personal, necesidad que aumenta cuando el tratamiento de la información incluye una transmisión de estas características. Si la transferencia estaba prevista antes de realizar el tratamiento, la referencia a dicha transmisión se realizará en la notificación de creación del fichero. Si la necesidad de transmitir información a esos niveles se genera una vez creado el fichero, deberá modificarse la inscripción que creaba el fichero. La notificación se realizará siguiendo el procedimiento ordinario establecido por el propio reglamento, sin que para estos casos se exijan requisitos específicos[3003].

Por otro lado, el reglamento reconoce la capacidad del Director de la Agencia de suspender temporalmente una transferencia a un país que presenta un nivel adecuado de protección si se dan una serie de circunstancias, fundamentalmente cuando se haya constatado, o haya indicios racionales, de que el importador concreto que recibirá la información ha vulnerado los principios de protección de datos[3004]. La suspensión deberá ajustarse al procedimiento establecido en el propio reglamento al respecto[3005]. Como se dijera más adelante, debería plantearse la posibilidad de aplicar esta facultad de suspender la transmisión a los casos en que el movimiento se va a realizar dentro del territorio del EEE. Si bien se ha reconocido que estos movimientos no tienen en el RDLOPD la consideración de transferencias internacionales, no hay que dejar de valorar que también en este tipo de transferencias el importador puede presentar unas circunstancias justificativas de la suspensión.

[3001] Artículo 20.2 LOPD: "*Las disposiciones de creación o de modificación de ficheros deberán indicar: (...)*
e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros".

[3002] Artículo 26.2 LOPD: "*Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente (...) las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros*".

[3003] Artículo 130 y siguientes.

[3004] Artículo 69 RDLOPD: "*1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:*
a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.
b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.
2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.
En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea". ÁLVAREZ RIGAUDIAS, "Las transferencias internacionales…", cit., 2010, p. 1.832.

[3005] Artículo 141 y siguientes RDLOPD.

B) En segundo lugar, en los casos en que la transmisión requiere de una autorización, por realizarse a un país que no presenta un nivel adecuado de protección, la capacidad de control del Director de la Agencia aumenta, como no podía ser de otra manera. Permanecen vigentes la señalada obligación de notificar la transferencia al registro y la posibilidad de suspender la operación. Esta última facultad, en este tipo de transmisiones, cuenta con un mayor campo de actuación que cuando se trata de transferencias a países que guardan un nivel de protección adecuado. Puede darse la suspensión o incluso la denegación de la autorización cuando se constate que la situación del país de destino en relación a la protección de los derechos fundamentales no garantiza el cumplimiento del contrato o acuerdo que justifica la autorización; cuando el importador haya incumplido previamente las garantías prefijadas en este tipo de contratos; cuando existan indicios de que dichas garantías no serán respetadas; cuando haya indicios de que los mecanismos que aseguran el cumplimiento del contrato no son efectivos; y, cuando se estime que la transferencia pueda crear una situación de riesgo de daño a los titulares de los dato[3006]. A estos dos instrumentos de control se suma, evidentemente, la facultad de autorizar o no la transferencia que se pretende. En este caso, el reglamento exige que la solicitud de autorización esté acompañada por la documentación que refleje el cumplimiento de las garantías exigibles para la obtención de la autorización y el cumplimiento de los requisitos necesarios para la realización de la transferencia[3007]. Los primeros documentos parecen referirse a la copia del contrato pertinente o las reglas corporativas vinculantes y los documentos que acreditan que son vinculantes y que en caso de incumplimiento de las mismas podrán exigirse responsabilidades. Los segundos, por su parte, parecen concernir a las pruebas que determinan que se han cumplido con los principios generales de protección de datos.

C) En tercer lugar, en las transferencias que la Ley exceptúa de la aplicación del régimen general que regula la transferencia internacional de datos, las facultades de control disminuyen. En este caso no cabe exigir la autorización del Director de la Agencia. Por otro lado, tampoco puede suspenderse la transferencia. Tiene sentido esta regulación en la medida en que si se trata de operaciones que se realizan atendiendo a motivos que justifican su exención del régimen

[3006] Artículo 70.3 RDLOPD: "*En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:*
a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.
b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.
c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.
d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.
e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.
La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.
Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.
[3007] Artículo 137 RDLOPD.

general, no tiene lógica que la autoridad competente pueda suspender estas operaciones. El único instrumento de control en este tipo de transferencias lo constituye, por lo tanto, la obligación de notificar los movimientos. La consideración de estos supuestos como casos excluidos de la aplicación del régimen general que regula la transferencia internacional de datos podría llevar a entender que también la obligación de notificar estas operaciones queda exceptuada en estos casos, pues en el RDLOPD esta obligación se reconoce como elemento que compone dicho régimen general. Sin embargo, si se hace una interpretación más favorable a la protección del derecho a la autodeterminación informativa, puede entenderse que la obligación genérica que establece la LOPD de notificar las transferencias internacionales se aplica a todo tipo de movimientos de esta naturaleza. Se entiende aquí que esta interpretación es necesaria debido a que lleva a justificar el único sistema de control de este tipo de transmisiones. No hay que olvidar que estas operaciones responden a unos motivos determinados. La necesidad de que estos motivos sean expuestos y controlados es argumento suficiente para justificar la obligación de notificar estas transmisiones de datos. Evidentemente, cuando la notificación se produzca parece coherente que el Director de la Agencia tenga la facultad de exigir que se transmita la documentación necesaria que pruebe la concurrencia del motivo que justifica la exención del régimen general. Así lo dispone expresamente la Instrucción de la AEPD reguladora de las transferencias internacionales[3008]. Lo dicho no quita para que en un momento determinado las propias circunstancias que motivan la aplicación del régimen exceptuado lleven a justificar un retraso o prórroga en el ejercicio de esta obligación. Sin embargo, no puede admitirse como punto de partida que este tipo de transferencias no requieran de su notificación a la Agencia.

Se ha expuesto el sistema de control articulado por las normas. En principio, esta serie de facultades reconocidas a la AEPD han de constituir un entramado de instrumentos suficiente para garantizar que las transferencias de datos se realizarán, en todo caso, en un entorno seguro y respetando los principios y derechos que componen el derecho a la autodeterminación informativa. Sin embargo, más allá de lo que dispone la letra de la normativa, es interesante hacer un breve apunte al litigo creado en torno a la citada Instrucción, para exponer cuál es el verdadero alcance de la facultad de control de la AEPD.

La validez de esta Instrucción fue cuestionada ante los tribunales. La principal polémica la creaba el apartado segundo de la norma tercera, que facultaba a la Agencia, a la hora de inscribir la transferencia en el Registro, cualquiera que fuera el tipo de transmisión, a requerir al responsable las garantías necesarias de que esa operación se fuera a realizar respetando la letra de la Ley. En este sentido, habilitaba a la institución a solicitar, en todo tipo de transmisiones, la presentación de documentación referida tanto al cumplimiento de las garantías concretas

[3008] Norma cuarta Instrucción AEPD 1/2000, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos: "*1. Cuando la transferencia internacional tenga por destinatario una persona física o jurídica, pública o privada, situada en el territorio de un Estado no miembro de la Unión Europea, respecto del que no se haya declarado por la Comisión de las Comunidades Europeas la existencia de un nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo y el transmitente se funde en alguno de los supuestos comprendidos en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que aporte la documentación que justifique su alegación*".

relativas a la transferencia internacional como al cumplimiento de los principios y derechos que configuran la autodeterminación informativa[3009].

Los tribunales entraron a cuestionar la facultad de control otorgada en la Instrucción a la AEPD[3010]. Según los tribunales está justificado que en los casos en que la norma exige autorización del Director de la AEPD se le requiera al responsable que aporte los documentos citados. Sin embargo, en los supuestos en que esa autorización no es necesaria es cuestionable esa facultad de la Agencia. Se entiende que no se puede establecer una forma alternativa de control previo sobre esas transmisiones, pues lo que la LOPD hace en su articulado es, precisamente, liberar de ese control las transferencias realizadas a los países destinatarios que cuenten con un sistema de protección adecuado[3011]. Evidentemente, si en las transferencias realizadas a países que cuentan con un nivel adecuado de protección, y en los casos exceptuados del régimen general que regula las trasferencias, se establece la facultad de la Agencia de requerir la citada documentación, se estará configurando un sistema de control alternativo al de la autorización.

Señalan los tribunales que en los casos en que se exige una autorización estará justificado el requerimiento de documentación adicional dirigida a demostrar, como exige el propio articulado

[3009] Norma tercera Instrucción AEPD, 1/2000, 1 de diciembre del 2000, relativa a las normas por las que se rigen los movimientos internacionales de datos: *1. De conformidad con el artículo 26.2 de la Ley Orgánica 15/1999 cualquier persona o entidad que pretenda efectuar una transferencia internacional de datos deberá hacerlo constar expresamente al proceder a la notificación del fichero al Registro General de Protección de Datos.*
La notificación de la transferencia se efectuará en los términos que se contengan en el modelo normalizado aprobado a tal efecto por el Director de la Agencia de Protección de Datos, con expresa indicación del país al que se pretende efectuar la transferencia y de los motivos que, en su caso, la habilitan, conforme a lo dispuesto en el artículo 34 de la citada Ley Orgánica, para no recabar la autorización expresa del Director de la Agencia de Protección de Datos.
En caso de que la transferencia internacional se refiera a datos contenidos en un fichero ya inscrito en el Registro General de Protección de Datos, no constando la transferencia en la inscripción, el responsable del fichero deberá solicitar una modificación de la misma, notificando los extremos a los que se refiere el párrafo anterior.
Si se tratara de ficheros de titularidad pública, la transferencia deberá estar prevista en la norma de creación o modificación del fichero.
2. Recibida la notificación, la Agencia de Protección de Datos podrá requerir al responsable del fichero para que en el plazo de diez días aporte la documentación necesaria para completar la información relativa a la transferencia internacional contenida en aquélla, así como la identidad del receptor de la misma.
A tal efecto, podrá solicitarse del responsable del fichero o tratamiento que aporte la documentación que acredite el cumplimiento de la obligación a la que se refiere la Norma Segunda de esta Instrucción. En particular, si el responsable invocase la existencia de consentimiento del afectado a la transferencia, podrá solicitarse que acredite la prestación de ese consentimiento. Del mismo modo podrá exigirse que se acredite la existencia de una relación contractual con el afectado que motive la transferencia, si aquélla hubiera sido alegada.
Igualmente, se podrá solicitar del responsable del fichero que acredite los extremos a los que se refiere la Sección Segunda de la presente Instrucción.
Al requerirse la información a la que se refiere este apartado se indicará al responsable del fichero que, en caso de no ser aquélla aportada en el plazo de diez días, se le tendrá por desistido de su petición de inscripción o modificación, archivándose ésta.
3. Si con la documentación aportada no se acreditara el cumplimiento de los requisitos contenidos en la Ley Orgánica 15/1999, el Director de la Agencia de Protección de Datos, en ejercicio de las competencias que le atribuye dicha Ley Orgánica, denegará la inscripción o su modificación.
4. Contra las resoluciones del Director de la Agencia de Protección de Datos relativas a la inscripción o, en su caso, a la modificación de un fichero, cabrá interponer potestativamente recurso previo de reposición o recurso contencioso-administrativo ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional".
[3010] SAN 15 de marzo de 2002, refrendada por la STS 25 de septiembre de 2006.
[3011] SAN 15 de marzo de 2002, FJ. 4. DAVARA RODRÍGUEZ, "La Transferencia Internacional…", cit., 2006, p. 44.

de la Ley, que se cumplen con las "*garantías adecuadas*": garantías de que el país de destino o el propio destinatario presenta una protección adecuada para los datos de carácter personal, y garantías también de que se han respetado los derechos de los afectados. En alguna memoria de la AEPD se ha reconocido, que en los casos en que la autorización del Director de la Agencia es necesaria se puede requerir al exportador documentación que asegure que se han cumplido con las siguientes garantías: información al afectado sobre las circunstancias que rodean a la transferencia, consentimiento o causa que justifica su ausencia, certificación de que el responsable es una entidad domiciliada en España y que dicha entidad facilitará desde España los derechos de acceso, rectificación y cancelación, y garantía de que en el país de destino no se iban a emplear los datos con una finalidad diferente a los iniciales ni que se comunicarán dichos datos a terceros[3012]. Sin embargo, en los casos en que esta autorización no es requerida, entienden los tribunales que no es posible exigir estos requisitos, pues ello llevaría a articular "unos trámites o mecanismos de control de significación equivalente a la autorización previa que ha sido expresamente excluida por el legislador"[3013].

Si bien lo que señalan los tribunales puede tener sentido, se entiende aquí que una correcta interpretación del ordenamiento puede llevar a concluir que las previsiones de la Instrucción no son contrarias a Derecho. Si se atiende a la comentada norma tercera de la Instrucción se puede observar que la misma dispone que la Agencia "podrá" requerir al responsable para que aporte la documentación citada. No se trata de un sistema de control general, equivalente a la autorización, sino que constituye una facultad que se podrá ejercer en atención a las circunstancias concretas que presente cada transferencia. Partiendo de esta previsión, podría admitirse, en contra quizás de lo que ha marcado otra línea doctrinal que ha aplaudido la comentada cita jurisprudencial[3014], un sistema de control de las transferencias más riguroso que el descrito por los tribunales.

Cuando las transferencias se realizan a un país que presenta un nivel adecuado de protección, la posibilidad de exigir al exportador, en el momento en que se va a inscribir la operación en el Registro, la presentación de los documentos que demuestran que se han respetado los principios de protección de datos y derechos de los afectados podría justificarse de la siguiente manera. Si, como se ha visto, se reconoce la facultad del Director de la AEPD de suspender una transferencia cuando se dan determinadas circunstancias, a pesar de que ésta se realice a un país que cuenta con un nivel adecuado de protección, no se encuentra motivo para que en este tipo de movimientos la Agencia no pueda llevar a cabo la actividad de control señalada. La posibilidad de suspender la transmisión responde a la necesidad de garantizar un nivel de protección adecuado a los datos, tanto en la realización de la operación como en su posterior tratamiento en el país importador. Ese nivel de protección no sólo se reconoce atendiendo a circunstancias referentes al importador de los datos, sino que deberán tenerse en cuenta también si se han cumplido los principios y derechos que configuran el derecho a la autodeterminación informativa. No hay motivo, si se tiene en cuenta el riesgo intrínseco a toda transmisión al extranjero, para que esa facultad de control se adelante, también en los casos en

[3012] Memoria de la AEPD de 1999.
[3013] SAN 15 de marzo 2002, FJ 7.
[3014] DAVARA RODRÍGUEZ, "La Transferencia Internacional…", cit., 2006, p. 45.

que la transferencia se va a realizar a un país que cuenta con un nivel adecuado de protección, al momento anterior a la inscripción en el registro.

Cuando las transferencias se llevan a cabo en circunstancias que justifican la excepción del régimen general regulador de los movimientos internacionales, las posibilidades de control son, evidentemente, menores. Como se dijera más arriba, en estos supuestos no cabe la suspensión de la transferencia. Sin embargo, se ha justificado la necesidad de notificar estas operaciones a efectos de su inscripción. Siendo la notificación exigible, parece que, a pesar de lo señalado por los tribunales, la posibilidad de que al exportador se le exija la documentación que demuestra el cumplimiento de los citados principios y derechos puede tener justificación. Hay que tener en cuenta que este tipo de operaciones llevan sujeto un riesgo potencial de envergadura. La posibilidad de que, si las circunstancias lo permiten, el sujeto exportador pueda ser requerido en el sentido expuesto, garantiza que cuando menos la transferencia se llevará a cabo con cierto control del sujeto afectado. Otra cosa será que la situación concreta que justifica este tipo de transferencia haga que este requerimiento afecte de manera negativa a la consecución del objetivo que se persigue y que justifica la aplicación del régimen especial. En estos casos es razonable que no se pueda exigir al exportador el cumplimiento del requisito citado. Sin embargo, más allá de estos supuestos, no hay motivo alguno para que el principio de proporcionalidad juegue a favor de una interpretación favorable al derecho a la autodeterminación informativa.

La base jurídica de esta afirmación puede encontrarse en la misma LOPD. Reconoce la Ley la facultad de la AEPD de "*recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones*[3015]", entre las que se encuentra la de "*ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos (...)*"[3016]. Cabe considerar dentro de esta ayuda la aportación de la documentación que se estime necesaria para probar que existe una situación que garantiza una transferencia segura, bien a la hora de otorgar la autorización pertinente, o bien, en caso de que la autorización no sea necesaria, a la hora de anotar en el registro esta operación.

Desde un punto de vista más sustantivo no hay más que reiterar argumentos que ya se han dado. La transferencia internacional, sea cual sea la vía que se haya de seguir para llevarla a cabo, plantea situaciones especialmente peligrosas para el derecho a la autodeterminación informativa. Incluso cuando se trata de países que de inicio guardan un nivel de protección adecuado los riesgos son inminentes pues la movilidad de los datos hace que la capacidad de control por parte del titular se reduzca. Las posibilidades que abre la normativa de contratar y subcontratar, y volver a subcontratar, servicios en el exterior que conllevan la manipulación de datos, ha de justificar que en determinados casos se abra la puerta a la facultad de la AEPD de controlar que se cumplen las garantías que constituyen los principios que componen el derecho que aquí se analiza. Piénsese en la posibilidad de que se transfieran datos relativos a la salud fuera del Estado, aunque se trate de un país que guarda un sistema de protección equivalente. La necesidad de garantizar que antes de que la transmisión se produzca se han respetado los

[3015] Artículo 37.1.i) LOPD.
[3016] Artículo 37.1.l) LOPD.

derechos de los titulares de los datos parece evidente ante las particularidades que presenta la transferencia internacional de datos.

III.6. Las transferencias internacionales en el ámbito estrictamente sanitario.

En este apartado se analizarán los problemas que plantea la aplicación del régimen jurídico descrito hasta ahora a la transferencia internacional de datos sanitarios. Una interpretación amplia de la letra de la LOPD podría llevar a crear un flujo incontrolado de datos sanitarios por los sistemas de información de todo el mundo, por lo que será necesario entender la Ley de tal forma que el derecho a la autodeterminación informativa se vea limitado en la menor medida posible.

III.6.1. La necesidad de que se transfieran datos de salud a otros países.

En un mundo en el que la circulación de las personas es constante resulta necesario que los datos de salud vinculados a dichas personas también fluyan[3017]. La necesidad de que este tipo de información se transfiera entre diferentes estados es patente en diferentes sectores. En el ámbito laboral, policial o en sectores tan concretos y polémicos como la lucha antidopaje en el deporte los movimientos internacionales de datos de salud constituyen una herramienta necesaria. En este último caso, por ejemplo, muestras biológicas y resultados de pruebas realizadas sobre dichas muestras se transfieren entre organizaciones antidopaje que se encuentran tanto en el ámbito de la UE como fuera de él. Es evidente que en este supuesto, al tratarse además de información referida a personas de cierta relevancia pública por ser deportistas profesionales, la necesidad de manipular dicha información con cierta precaución es manifiesta. En este sentido, el Código Mundial Antidopaje hace especial hincapié en la necesidad de proteger la confidencialidad de los datos que se manipulan[3018]. La propia WADA (*World Anti-Doping Agency*) ha aprobado la Norma Internacional para la Protección de los Datos Personales y su Confidencialidad, en la que se reconoce la necesidad de proteger el derecho a la vida privada de los deportistas y la necesidad de que los datos referentes a los mismos se manipulen con ciertas garantías[3019]. En otro ámbito como el policial y judicial la necesidad de que se transmitan datos de salud entre diferentes estados queda patente en los textos que se han citado y que regulan estos sectores en el ámbito de la UE. El Convenio de Aplicación del Acuerdo de Schengen excluye, de inicio, la posibilidad de tratar datos sensibles[3020], si bien reconoce casos concretos en que la comunicación de los datos de salud entre países resulta necesaria para

[3017] SÁNCHEZ CARAZO y ABELLÁN, *Datos de Salud…,* cit., 2004, p. 78.
[3018] Artículo 14, *World Anti-Doping Code,* 2003.
[3019] Norma Internacional para la Protección de los Datos Personales y su Confidencialidad, 1 de junio de 2009. Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 3/2008, sobre el proyecto de norma internacional del Código Mundial Antidopaje para la protección de la intimidad, 1 de agosto de 2008; *Second Opinion 4/2009 on the World Anti-Doping Agency (WADA) International Standard for the Protection of Privacy and Personal Information, on related provisions ef the WADA Code ando n other privacy issues in the contexto f the fight against doping in sport by WADA and (nacional) anti-doping organizations*, 6 de abril de 2009. TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 98.
[3020] Artículo 94.3 Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, 19 de junio de 1990: "*(…) No se autorizarán otras anotaciones, en particular los datos enumerados en la primera frase del artículo 6 del Convenio del Consejo de Europa de 28 de enero de 1981 para la protección de las personas en lo referente al tratamiento informatizado de datos de carácter personal*".

facilitar la circulación de las personas. Es el caso, por ejemplo, en que se transmite de un lugar a otro documentación sobre la justificación de que un sujeto lleve consigo un medicamento o sustancia determinada[3021]. En el marco del Convenio que crea la Europol la posibilidad de emplear datos de salud se reconoce expresamente, si bien se limita a fines muy concretos[3022]. Lo mismo ocurre con el Convenio que crea Eurojust[3023].

En lo que aquí interesa, en el ámbito sanitario son indudables las bondades de la creación de un flujo de información transfronterizo en un mundo en el que las cuestiones vinculadas a la salud tienen una dimensión cada vez más global[3024]. Es evidente que la circulación de este tipo de datos plantea escenarios que han de valorarse positivamente: la posibilidad de que una persona pueda ser asistida en cualquier punto del planeta empleando toda la información posible sobre ella, la capacidad de crear redes de información sanitaria que faciliten proyectos de investigación llevados a cabo por entidades situadas en distintos países, la posibilidad de luchar contra enfermedades que traspasan las fronteras de los estados o la posibilidad de que un facultativo realice consultas concretas sobre la enfermedad de una persona a profesionales situados en otro país son un botón de muestra de las alternativas que plantea la transferencia internacional de datos[3025].

La necesidad de transmitir información sanitaria a otros estados se ve hoy día satisfecha, en la medida en que las TIC facilitan que este flujo de datos a nivel internacional pueda llevarse a cabo de manera ágil, sencilla y también segura. Los datos sanitarios, cualquiera que sea el formato, pueden ser transmitidos a cualquier punto del planeta. Sin embargo, es evidente que estas operaciones no pueden realizarse sin atender a una serie de reglas y criterios. El principal

[3021] Artículo 75 Convenio de Aplicación del Acuerdo de Schengen, de 14 de junio de 1985, 19 de junio de 1990: "*1. Por lo que se refiere a la circulación de viajeros con destino a territorios de las Partes contratantes o por dichos territorios, las personas podrán transportar los estupefacientes y sustancias sicotrópicas que sean necesarias en el marco de un tratamiento médico, siempre que al efectuarse un control puedan presentar un certificado expedido o legalizado por una autoridad competente del Estado de residencia*
2. El Comité ejecutivo establecerá la forma y el contenido del certificado contemplado en el apartado 1 y expedido por una de las Partes contratantes, y en particular los datos relativos a la naturaleza y la cantidad de los productos y sustancias y a la duración del viaje.
3. Las Partes contratantes se comunicarán mutuamente qué autoridades son competentes para la expedición o legalización del certificado contemplado en el apartado 2".

[3022] Artículo 10.1 Convenio basado en el artículo K.3 del Tratado de la Unión Europea por el que se crea una oficina europea de policía (Convenio Europol), hecho en Bruselas el 26 de julio de 1995: "*(...) La recogida, el almacenamiento y el tratamiento de los datos que se enumeran en la primera frase del artículo 6 del Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal sólo se autorizarán cuando sean estrictamente necesarios para la finalidad del fichero de que se trate y cuando tales datos completen otros datos personales introducidos en ese mismo fichero. Queda prohibido seleccionar una categoría particular de personas a partir únicamente de los datos de la primera frase del artículo 6 del Convenio del Consejo de Europa de 28 de enero de 1981, en vulneración de las normas de finalidad citadas*". Informe de Actividad 1998-2002 de la Autoridad de Control Común de EUROPOL.

[3023] Artículo 15.4 Decisión del Consejo 2002/187/JAI, 28 de febrero de 2002, por la que se crea Eurojust para reforzar la lucha contra las formas graves de delincuencia, DO nº L 63/1, 6 de marzo de 2002: "*Eurojust sólo podrá tratar datos personales, tanto por medios informatizados como no informatizados, sobre el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, así como sobre la salud o la vida sexual de las personas, si dichos datos son necesarios para las investigaciones nacionales de que se trate y para la coordinación en Eurojust*".

[3024] PONS RAFOLS, "La salud como objeto…", cit., 2010, p. 27.

[3025] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los Historiales Médicos Electrónicos (HME), 15 de febrero de 2007.

problema que surge en relación a este tipo de movimientos lo constituye la necesidad de configurar una regulación que garantice que los derechos fundamentales de los titulares de los datos, fundamentalmente el derecho a la autodeterminación informativa, se van a respetar cuando las transferencias se lleven a cabo. Hay que tener en cuenta que un flujo incontrolado de este tipo de información conllevaría una serie de riesgos de envergadura. Por un lado, crearía un entorno en el que los datos podrían ser empleados de manera torticera, para conseguir fines que nada tienen que ver con la salvaguarda de intereses privados o comunes legítimos. Por otro, abriría la puerta a un flujo de datos de salud en el que sería fácil su alteración o pérdida. La necesidad de que la regulación de estas operaciones genere un marco seguro en el que poder realizar los movimientos internacionales de datos es obvia.

En este sentido, las leyes no definen un régimen específico dedicado a regular las transferencias internacionales de los datos sanitarios. Es más, no hace distinción alguna a la hora de regular las transferencias entre datos comunes y datos que son objeto, en la propia LOPD, de una protección especial. La transferencia internacional de datos sanitarios no es un punto que haya sido estudiado extensamente por la doctrina. Tampoco la jurisprudencia ni la AEPD han tratado esta cuestión de manera expresa. Lo cierto es que se trata de una materia que, si bien tiene gran relevancia, no plantea demasiados problemas específicos más allá de los que se han ido sugiriendo a lo largo de este trabajo. En todo caso, cabe hacer mención a una serie de cuestiones que precisan aclaración para tener una perspectiva general de los supuestos en que pueden transferirse los datos sanitarios.

III.6.2. La transferencia de datos de salud con fines sanitarios. Un supuesto exceptuado del régimen general que regula los movimientos internacionales.

El punto de partida a la hora de determinar de qué forma se pueden llevar a cabo transferencias internacionales de datos sanitarios ha de ser la única referencia que se hace en la Ley al ámbito de la salud. Señala la Ley que queda fuera del régimen general que regula la figura del movimiento internacional de datos la transferencia realizada "*para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamiento médico o la gestión de servicios sanitarios*"[3026]. Partiendo de esta disposición pueden distinguirse diferentes supuestos de transferencia internacional de datos sanitarios.

Ha habido quien ha criticado el hecho de que se pueda exceptuar de la aplicación del régimen general la transferencia de datos que están sometidos en la Ley a un régimen especial de protección[3027]. Sin embargo, como se puede deducir de la letra de la citada disposición, en lo referente a los datos de salud hay un ámbito en el que los movimientos internacionales pueden realizarse con cierta libertad, sin necesidad de recabar autorización del Director de la AEPD, independientemente de que el país importador guarde un nivel de protección adecuado o no. Más allá de este ámbito toda transmisión de este tipo de datos ha de regirse por el régimen

[3026] Artículo 34.c) LOPD.

[3027] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 377; LEGALIA, *La Protección...*, cit., 2002, p. 108, "considera injustificado que, tratándose de una información calificada por el artículo 7 de la LOPD como especialmente protegida, pueda ser transmitida a países que no proporcionan un nivel de custodia equiparable, eludiendo incluso la autorización del Director de la Agencia".

general establecido en las normas, dependiendo de si el país de destino cuenta con un nivel de protección adecuado o no. Es necesario, por lo tanto, antes de nada, definir ese campo que queda exceptuado del régimen general. Para ello, será necesario comparar el contenido de la LOPD con las disposiciones recogidas en otras normas.

En la Directiva europea se reconoce la posibilidad de aplicar la excepción cuando "*la transferencia sea necesaria para la salvaguardia del interés vital del interesado*"[3028]. La redacción de este artículo parece restringir el ámbito de aplicación a casos verdaderamente excepcionales. Algún autor, siguiendo lo que ha dispuesto la Directiva, ha entendido que esta transferencia se limitará a los casos vinculados a un "interés médico grave"[3029]. Ciertamente, si se realiza la interpretación sujetándose de manera estricta a la letra de la norma, se entenderá que la excepción tiene aplicación sólo cuando esté en juego la vida de las personas[3030]. Por su parte, y en la misma línea de la Directiva, de la Recomendación del Consejo de Europa que regula la protección de los datos sanitarios se deduce que la excepción se aplicará sólo en casos de "emergencia"[3031]. Si se tiene en cuenta que la Directiva recoge las garantías mínimas que todo estado deberá respetar en la protección de los datos de carácter personal, se podría llegar a entender que la normativa interna no puede ser objeto de una interpretación más amplia que la que propone la norma comunitaria. Sin embargo, ya se ha visto que la LOPD dispone que la excepción podrá aplicarse en un sentido más amplio que el dispuesto en la norma europea, no sólo en casos de extrema urgencia sino cuando el objetivo sea la asistencia sanitaria, la prevención de enfermedades y la gestión de estos servicios[3032]. Parece evidente que la redacción empleada por la norma estatal abraza un número mayor de supuestos que la Directiva[3033]. La LORTAD por su parte establecía un régimen diferente al establecido en la LOPD. Señalaba la Ley ya derogada que la excepción podía aplicarse cuando tuviera por objeto "*el intercambio de datos de carácter médico entre facultativos o instituciones sanitarias y así lo exija el tratamiento del afectado, o la investigación epidemiológica de enfermedades o brotes epidémicos*"[3034].

Se entiende aquí que la solución ha de venir de una interpretación intermedia entre lo dispuesto por ambas normas. En primer lugar, no parece que se pueda limitar el ámbito de aplicación de esta excepción a los casos en que la vida de las personas está en juego. El principio de proporcionalidad exige que en otros casos de urgencia, aunque no esté en peligro la vida de las personas, pueda aplicarse la excepción. Hay que tener en cuenta que las transferencias no constituyen, simplemente, una vía para obtener información que puede ayudar a entender la enfermedad de una persona en concreto, sino que puede ser una vía para evitar posibles enfermedades o problemas, por ejemplo, en el caso de reacciones alérgicas a determinados medicamentos. Limitar los supuestos de transferencia a los casos en que está en

[3028] Artículo 26.1.e) Directiva 95/46/CE.
[3029] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 191
[3030] Considerando 31 Directiva 95/46/CE, parece definir ese interés vital como "*interés esencial para la vida"*.
[3031] Artículo 11.5 R (97) 5: *"Salvo en caso de emergencia o de una transferencia a la que el titular de los datos haya dado su consentimiento informado, se deben tomar medidas apropiadas para asegurar la protección de los datos médicos transferidos de un país a otro (...)*".
[3032] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 600.
[3033] BUISÁN GARCÍA, "Movimiento Internacional…", cit., 2008, p. 576.
[3034] Artículo 33.c) LORTAD.

juego la vida de las personas podría cerrar la puerta a operaciones que son necesarias para salvaguardar la salud. En segundo lugar, tampoco parece que se pueda plantear la excepción en términos tan amplios como lo hace la LOPD. La transferencia internacional de datos sanitarios estará justificada cuando sea necesaria para garantizar la integridad física y psíquica de un ciudadano, independientemente de la voluntad del mismo. Es decir, la solución deberá venir de la estricta aplicación del principio de proporcionalidad en cada caso, atendiendo a criterios puramente médicos. Da pie a realizar esta interpretación el hecho de que la propia LOPD emplee la expresión "*cuando (…) sea necesaria*". No se trata de limitar esos supuestos sólo a los casos en que la vida de un ciudadano está en juego, sino que ha de entenderse que se aplica a los casos en que la salud de éste lo requiera[3035]. Cuando no sea necesaria habrá que estar a cada caso, para ver si es necesaria o no la autorización del Director de la AEPD. Y, sobre todo, esta excepción sólo se deberá aplicar, independientemente de que se esté en juego la vida de una persona o no, cuando las otras formas de realizar transferencias internacionales no pueden ser aplicadas.

Se ha señalado que esta excepción no puede interpretarse de forma especialmente amplia. Así, se ha negado la posibilidad de justificar este tipo de transferencias cuando se hacen, en el ámbito sanitario, con fines exclusivamente administrativos[3036]. Lo cierto es que la redacción de la Ley hace referencia expresa a la "gestión de servicios sanitarios", por lo que sería fácilmente deducible que los fines administrativos tienen también aplicación aquí. Sin embargo, se entiende que este concepto hay que entenderlo en un sentido restrictivo, de tal forma que este tipo de gestiones sólo podrán justificar una transferencia fuera del régimen general cuando esté vinculada a un tratamiento sanitario. La mera finalidad administrativa no puede justificar la excepción.

Se han planteado dudas también a la hora de aplicar la excepción con fines sanitarios pero vinculados a la investigación[3037]. En esta línea, desde el Grupo de Trabajo del artículo 29 de la Directiva se ha indicado que la aplicación de la excepción ha de aplicarse exclusivamente en beneficio del interesado. Esta afirmación negaría la posibilidad de justificar estas transferencias cuando el fin es la consecución del interés general, representado por ejemplo en actos de investigación[3038]. La LOPD no hace referencia expresa a estos supuestos. La LORTAD incluía en la excepción los casos de "*investigación epidemiológica o brotes epidémicos"*. El hecho de que de la Ley actual se haya excluido esta referencia parece revelador Sin embargo, no es menos cierto que la actual norma se refiere a la posibilidad de aplicar la excepción cuando la finalidad es meramente preventiva, lo cual podría llegar a englobar los supuestos vinculados a la investigación, fundamentalmente cuando se trata de estudios epidemiológicos. En relación con la investigación en el ámbito de la salud, desde la OCDE se ha puesto de manifiesto que la protección de los datos sanitarios constituye la principal barrera para el flujo de información

[3035] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, para la Interpretación Común del artículo 26.1 de la Directiva 95/46/CE de 24 de octubre de 1995, de 25 de noviembre de 2005.
[3036] Memoria de la AEPD 2004, en la que parece subrayarse la idea de que la finalidad ha de ser estrictamente médica.
[3037] COUDERT, "Transferencias Internacionales…", cit., 2007, p. 446.
[3038] SERRANO DE PABLO VALDENEBRO, "Las Transferencias Internacionales…", cit., 2008, p. 600. Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, relativo a una interpretación común del artículo 26, apartado 1, de la Directiva 95/46/CE de 24 de octubre de 1995, 25 de noviembre de 2005.

necesario para avanzar en dichas labores de investigación[3039]. Si bien es cierto que esa perspectiva parece rebajar la relevancia de la protección de un derecho fundamental como la autodeterminación informativa, no es menos cierto que subraya la importancia de la investigación en el sector sanitario, importancia que no puede ser desatendida o ignorada. En gran medida, como se ha expuesto en numerosas ocasiones en este trabajo, la prevención exige necesariamente la realización de investigaciones. En casos concretos en que estas investigaciones responden a motivos de urgencia, como puede ser el supuesto de una epidemia a escala internacional, la realización de estas actividades pasa porque se facilite el flujo de la información sanitaria, incluso la que se vincula a personas determinadas. De esta forma, no parece que se pueda rechazar de inicio la posibilidad de aplicar la excepción que ahora se analiza a este tipo de tareas. Desde la OCDE se señala como elemento fundamental el que se adopten las medidas técnicas oportunas para que las transferencias se realicen de forma segura, resaltando la importancia que pueden tener en este sentido los Códigos de Conducta y los contratos como instrumentos que favorecen la salvaguarda del derecho a la autodeterminación informativa en los países importadores[3040].

La aplicación de la excepción que ahora se analiza puede llegar a plantear una situación especialmente comprometida para el titular de los datos. Como se ha dicho más arriba, en las transferencias internacionales de datos deberán respetarse, al igual que en cualquier otra operación, los principios y derechos que configuran el derecho a la autodeterminación informativa, fundamentalmente los derechos a consentir y a ser informado. En el caso de los datos sanitarios ya se ha visto que la finalidad que impulse un tratamiento concreto de los datos determinará si los citados derechos se exceptúan o no. Así, el empleo de la información con el objetivo de salvaguardar la salud de las personas es argumento suficiente para flexibilizar e, incluso, excepcionar la exigencia de recabar el consentimiento del titular de los datos o la necesidad de informar a este último de la manipulación que se va a llevar a cabo de sus datos. Pues bien, se acaba de ver que esa misma finalidad puede llevar a que el régimen general que regula las transferencias no sea aplicable y que los datos de salud puedan ser transmitidos a países que no guardan un nivel de protección adecuado sin necesidad de la autorización del Director de la AEPD. Como se puede deducir, las facultades de control sobre los datos en las transferencias de datos de salud en los casos en que la excepción es aplicada quedan reducidas al mínimo. Un ciudadano, por lo tanto, puede encontrarse con que sus datos han sido trasladados a un país que no guarda un nivel de protección equivalente al que aquí se reconoce sin que haya otorgado consentimiento alguno, sin que haya sido informado y sin que la Agencia haya autorizado dicha operación. En principio, se ha entendido aquí, la notificación de estas transferencias a la AEPD es preceptiva. Sin embargo, hay casos en que debido a la urgencia de la situación no podrá llevarse a cabo. La situación que deja esta posibilidad en lo que al derecho a la autodeterminación informativa es preocupante, pues favorece que este tipo de información pueda ser manipulada en el país importador con total libertad y sin que el titular tenga

[3039] Documento de Trabajo de la OCDE "*Data Protection in Transborder Flows of Health Research Data",* 10 de diciembre de 1999.
[3040] Documento de Trabajo de la OCDE "*Data Protection in Transborder Flows of Health Research Data",* 10 de diciembre de 1999.

conocimiento alguno de lo que se está haciendo con datos que revelan esferas íntimas de su personalidad.

Será necesario adoptar las medidas necesarias para que este tipo de situaciones sólo se produzcan cuando sea imprescindible. En primer lugar, el principio de proporcionalidad deberá aplicarse de manera rigurosa a la hora de aplicar la excepción del artículo 34, de tal forma que se emplee sólo en los casos en que sea estrictamente necesario. Y en segundo lugar, como garantía mínima necesaria en la protección del derecho a la autodeterminación informativa, será necesario que el exportador de datos notifique cuando sea posible de la transferencia a la Agencia e informe del particular al titular de los datos.

III.6.3. Otros supuestos de transferencia de datos de salud.

La transferencia de los datos de salud puede llevarse a cabo, como se acaba de ver, en aplicación de la excepción citada. Se plantea ahora si es posible realizar dichas transmisiones a otros estados empleando los demás tipos de movimiento internacional de datos. Pueden darse dos situaciones diferentes: A) que pueda aplicarse una de las excepciones recogidas en el artículo 34 distinta a la basada en los motivos sanitarios, y B) que no pueda aplicarse excepción alguna.

A) En primer lugar, y siguiendo con los supuestos exceptuados del régimen general regulador de las transferencias, cabe preguntarse si más allá de la excepción referida al ámbito sanitario, es posible aplicar a los datos de salud las demás excepciones que se recogen en el artículo 34 de la Ley, o si por el contrario hay que entender que en el caso de los datos considerados sensibles no se puede emplear ese sistema de excepciones. De inicio, parece que la normativa plantea su aplicación sin ningún tipo de matización. Se entiende aquí que esta regulación puede cuestionarse.

Primero, hay que recordar que se ha ido otorgando a lo largo del articulado de la Ley un nivel especial de protección, entre otros, a los datos de salud. Este mismo planteamiento podría aplicarse en lo que toca a las transferencias internacionales de datos. En este sentido, la Recomendación del Consejo de Europa reguladora de la protección de datos médicos reconoce la posibilidad de aplicar exclusivamente la excepción referida al consentimiento del propio afectado, se entiende que consentimiento expreso, sin hacer mención a ningún supuesto más[3041]. No hay que olvidar, en esta línea, lo que se decía sobre la posibilidad de realizar una interpretación amplia del citado precepto. El que se haya de entender este artículo en un sentido restrictivo favorece la interpretación que aquí se realiza.

Y segundo, no hay que olvidar que en el análisis que se ha estado realizando hasta ahora se ha puesto de manifiesto que los límites al derecho a la autodeterminación informativa, cuando se trata de datos de salud, han de interpretarse de manera restrictiva. Es decir, la limitación de este

[3041] Artículo 11.4 R (97) 5: *"Salvo que la ley nacional disponga otra cosa, el flujo transfronterizo de datos médicos a un Estado que no asegura la protección de acuerdo con la Convención y con esta recomendación, el flujo no debe tener lugar a menos que: (...)*
b) el afectado haya dado su consentimiento".

derecho a favor de un tratamiento de datos determinado se realiza siempre cuando está en juego un bien jurídico de entidad. Evidentemente, las excepciones que se plantean en el artículo 34 constituyen una limitación a dicho derecho, en la medida en que suponen una minoración de las garantías que salvaguardan la capacidad de control sobre los datos. Necesariamente, esta relajación de la protección debe estar justificada por el hecho de que entran en juego esos bienes jurídicos de entidad. Los intereses que pueden justificar una limitación de la autodeterminación informativa cuando se refiere a los datos de salud, no son los mismos que justifican la limitación de dicho derecho cuando concierne a información que no tiene en la Ley la consideración de sensible. En este sentido, parece lógico pensar que los supuestos en que se justifica el movimiento internacional de datos sanitarios sin autorización previa, se limitarán a casos muy puntuales en que hay un bien jurídico de especial envergadura en juego. Esta cuestión se refleja fundamentalmente en las transferencias que se deban realizar con el fin de ejecutar un contrato o para la adopción de medidas precontractuales, o con el fin de celebrar un contrato[3042]. Al hablar de la cesión se había visto que si bien en el caso de los datos comunes la configuración de un contrato podía ser argumento para exceptuar el derecho al consentimiento, no ocurría lo mismo en relación a los datos relativos a la salud. Siendo esto así, no tiene lógica alguna que ese mismo fin permita la realización de una transferencia internacional a un país que no guarda un nivel de protección adecuado sin necesidad de control previo alguno. Hay que tener en cuenta que este tipo de transferencias constituirían un límite al derecho, incluso mayor que la excepción al consentimiento que se reconoce en las cesiones, pues permitiría el traslado de los datos a un país en que la información podría llegar a ser manipulada sin control alguno. Siendo esto así, dejaría de ser coherente que no se aplique a los datos de salud el límite previsto en la regulación de las cesiones para los datos comunes y que, por el contrario, sí se aplique la excepción comentada en las transferencias internacionales.

B) Se ha visto que en el ámbito estrictamente sanitario las transferencias internacionales podrán realizarse en algunas ocasiones sin atender al régimen general que regula este tipo de operaciones. Sin embargo, más allá de estos supuestos será necesario que las transmisiones de la información concerniente a la salud de las personas siga el régimen que se ha expuesto en los apartados precedentes, de tal forma que se garantice que la transferencia se realizará en un entorno seguro y que el importador empleará la información de manera respetuosa con el derecho a la autodeterminación informativa. En segundo lugar, por lo tanto, cabe analizar los casos en que los datos de salud se transfieren atendiendo al régimen general que regula las transferencias internacionales de datos. Habrá que analizar en el caso concreto si el movimiento se realiza a un país sobre el cuál bien la AEPD o bien la Comisión Europea han declarado que guarda un nivel de protección adecuado o equiparable al que disponen la LOPD y la Directiva europea, o si, por el contrario, la transferencia se lleva a cabo a un país importador en el que no existe dicho nivel de protección, por lo que será necesaria una autorización del Director de la Agencia. Para ambos casos la Recomendación del Consejo de Europa dispone expresamente la necesidad de que se garantice que el importador respetará fundamentalmente el principio de

[3042] Artículo 34.f) y g) LOPD.

finalidad y que no remitirá la información fuera del ámbito preestablecido[3043]. En este tipo de transferencias el hecho de que los datos sean objeto de una especial protección en el ordenamiento no altera el procedimiento que se ha de seguir para llevarlas a cabo. Sin embargo, en la práctica, esta circunstancia sí deberá ser tenida en cuenta a la hora de aprobar o no una transferencia.

En el primer caso, señala el ordenamiento que el nivel adecuado de protección se establecerá atendiendo, entre otros factores, a la naturaleza de los datos. Efectivamente, la determinación del nivel adecuado de protección de los datos pasa porque en el régimen jurídico que presenta el país importador se establezca, como se hace en la LOPD, una protección reforzada o especial para la información sensible, en este caso de salud. Disponen también las normas, que el régimen adecuado se deducirá atendiendo a las normas profesionales. En el ámbito sanitario la existencia de códigos de conducta y protocolos de actuación vinculantes y de contenido exigible jurídicamente ha de ser tenida en cuenta. En las transferencias internacionales a países que cuentan con un nivel de protección adecuado la transmisión de la información sanitaria estará sujeta exclusivamente a la obligación de notificación. Más allá de este requisito las transferencias podrán realizarse como si de una cesión se tratara, atendiendo a los principios que rigen esta operación: consentimiento e información, fundamentalmente. En este espacio en el que se cuenta con un nivel adecuado de protección, la libertad a la hora de realizar las transferencias facilita la creación de flujos de información que, en el ámbito sanitario concretamente, abre la puerta a posibilidades que se han expuesto y que han de ser valoradas positivamente. En este sentido, la Recomendación del Consejo de Europa que regula el tratamiento de datos médicos afirma que el movimiento de este tipo de información dentro de la UE y entre los países que guardan un nivel de protección de la información equiparable no ha de estar sujeta a controles específicos[3044].

A pesar de que las transmisiones dentro de la UE no se consideren en el RDLOPD transferencias internacionales, hay que destacar que son múltiples los proyectos que en este ámbito se plantean en aras de mejorar la salud de los ciudadanos, y que conllevan la transmisión de los datos a otros países miembros de la Unión. En la actualidad, la principal referencia en relación a esta cuestión la constituye la propuesta de Directiva del Parlamento Europeo y del

[3043] Artículo 11.5 R (97) 5: *"Salvo en caso de emergencia o de una transferencia a la que el titular de los datos haya dado su consentimiento informado, se deben tomar medidas apropiadas para asegurar la protección de los datos médicos transferidos de un país a otro, y en particular:*
a) la persona responsable de la transferencia debe indicar al destinatario los fines específicos y legítimos para los que se recogieron los datos, así como las personas u organismos a los que éstos pueden comunicarse
b) salvo que la legislación nacional disponga otra cosa, el destinatario debe comprometerse ante la persona responsable de la transferencia a respetar los fines específicos y legítimos que éste último ha aceptado, y a no comunicar los datos a personas u organismos distintos de los indicados por la persona responsable de la transferencia".

[3044] Artículo 11 R (97) 5: *"2. No debe someterse a condiciones especiales de protección de la intimidad el flujo transfronterizo de datos médicos a un Estado que ha ratificado la Convención para la Protección de los Individuos en relación al Tratamiento Automatizado de Datos Personales, y que dispone de legislación que proporciona al menos una protección equivalente de los datos.*
3. Donde la protección de los datos médicos pueda considerarse en línea con el principio de protección equivalente sentado por la convención, no se debe aplicar restricción alguna al flujo transfronterizo de datos médicos a un Estado que no haya ratificado la Convención, pero que disponga de normas legales que aseguren una protección acorde con los principios de tal Convención y de esta recomendación".

Consejo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza[3045]. Después de muchos años se afrontan en la UE los diversos problemas que se generan a la hora de dar una asistencia sanitaria eficiente a las personas que circulan entre los distintos países que la conforman. En lo aquí interesa, la Directiva hace referencia a los problemas que crean los principales instrumentos que han de ser aplicados a escala de la UE para que esa asistencia transfronteriza pueda llevarse a cabo. La posibilidad de que una receta emitida en un país pueda ser leída y autentificada en otro, la necesidad de que las tecnologías empleadas en los distintos países sean compatibles para que, entre otras cosas, la transmisión de datos y su posterior tratamiento pueda llevarse a cabo de manera eficiente, son ejemplos de lo dicho. Como no podía ser de otra manera, la propuesta atiende a la importancia de que en todo este proceso sea necesario garantizar en todo caso el derecho de los ciudadanos a la autodeterminación informativa. En este sentido, realiza una remisión expresa a la Directiva europea reguladora de la protección de datos[3046].

En relación a proyectos más concretos los problemas son los mismos y son puestos de manifiesto en diversos documentos. Tanto la telemedicina entendida en un sentido estricto[3047], o la creación de una historia clínica electrónica única a nivel europeo[3048], como los demás proyectos que se puedan incardinar en el ámbito de la salud electrónica exigen de la transferencia de datos sanitarios, y una de las principales preocupaciones desde la UE no deja de ser la de crear una red de datos segura[3049]. Se trata de aprovechar las nuevas tecnologías a la hora de realizar transferencias de datos a otros países para poder otorgar un servicio sanitario eficiente. En el ámbito de la prevención también son distintos los proyectos que se plantean en el espacio europeo. Es referencia obligada la creación de una red de vigilancia epidemiológica a escala europea que, evidentemente, conlleva la transmisión de datos de salud[3050]. En relación a

[3045] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, COM (2008) 414 final, 2 de julio de 2008.

[3046] Artículo 3.1.a) Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, COM (2008) 414 final, 2 de julio de 2008.

[3047] Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones, "La Telemedicina en beneficio de los pacientes, los sistemas sanitarios y la sociedad", COM (2008)689 final, 4 de noviembre de 2008.

[3048] MÉJICA GARCÍA, *El Enfermo Transparente…,* cit., 2002, p. 66.

[3049] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones, "La salud electrónica-hacia una mejor asistencia sanitaria para los ciudadanos europeos: Plan de acción a favor de un Espacio Europeo de la Salud Electrónica", COM (2004) 356 final, 30 de abril de 2004. Puede realizarse una lectura exhaustiva de los proyectos en materia de eSalud en el ámbito europeo en http://ec.europa.eu/information_society/tl/qualif/health/index_es.htm.

[3050] Artículo 4 Decisión del Parlamento Europeo y del Consejo 2119/98/CE, 24 de septiembre de 1998, por la que se crea una red de vigilancia epidemiológica y de control de las enfermedades transmisibles en la Comunidad, DO nº L-268, 3 de octubre de 1998: "*Cada una de las estructuras y/o autoridades contempladas en el párrafo segundo o tercero, según sea el caso, del artículo 1 comunicará a la red comunitaria:*
a) las informaciones relativas al brote o reaparición de casos de enfermedades transmisibles contempladas en la letra a) del artículo 3 en el Estado miembro al que pertenezca dicha estructura y/o autoridad, junto con la información relativa a las medidas de control aplicadas;
b) toda información útil relativa a la evolución de las situaciones de epidemia sobre las que esté encargada de recoger información;
c) información sobre fenómenos epidemiológicos infrecuentes o nuevas enfermedades transmisibles de origen desconocido;
d) toda información pertinente que obre en su poder:
- sobre casos de enfermedades transmisibles incluidas en las categorías enumeradas en el anexo, o

enfermedades concretas la lucha contra el Sida incluye también proyectos de alcance global transfronterizo que implica la transmisión de datos, en este caso especialmente sensibles[3051].

En el segundo caso, cuando la transferencia se va a llevar a cabo a un Estado que no presenta un nivel de protección equiparable y requiere de una autorización, el hecho de que los datos a transmitir sean datos sanitarios también afecta a la hora de aprobar o no las transferencias. No es extraño que se remitan datos sanitarios a países que no guardan un nivel adecuado de protección. La mayoría de las veces estas operaciones se han enmarcado en la relación creada entre una empresa estatal y otra empresa, o una sucursal de la primera, que se encargará en nombre de la exportada de la gestión de recursos humanos[3052], o en transmisión de ficheros de una empresa aseguradora a una entidad que tramitará determinados servicios a los asegurados desde un país que no presenta un nivel adecuado de protección[3053]. La Recomendación del Consejo de Europa reconoce la posibilidad de transmitir datos de salud a un país que no presente garantías adecuadas cuando esas garantías se prevén en instrumentos como contratos[3054]. A la hora de dar la autorización, el Director de la AEPD deberá contemplar si el contrato, acuerdo o las reglas corporativas vinculantes establecen un nivel de protección acorde al estatus que los datos de salud tienen en la LOPD, fundamentalmente en relación a las medidas de seguridad a adoptar. Como se puede imaginar, no es lo mismo autorizar la transferencia de datos que de inicio no se refieren a aspectos especialmente relevantes de la vida de una persona, que permitir la transmisión de datos sanitarios. También habrá que atender en estos casos al dato sanitario concreto, pues tampoco es lo mismo transmitir información sobre un proceso gripal que una afección por el VIH.

- sobre nuevas enfermedades transmisibles de origen desconocido que aparezcan en terceros países;
e) la información relativa a los mecanismos y procedimientos existentes o propuestos destinados a prevenir y controlar las enfermedades transmisibles, en particular en situaciones de emergencia;
f) todos los elementos de valoración que puedan ayudar a los Estados miembros a coordinar sus esfuerzos de prevención y control de enfermedades transmisibles, incluidas las medidas de lucha aplicadas". En el mismo sentido, Decisión de la Comisión 2009/547/CE, 10 de julio de 2009, por la que se modifica la Decisión 2000/57/CE, relativa al sistema de alerta precoz y respuesta para la vigilancia y control de las enfermedades transmisibles en aplicación de la Decisión 2119/98/CE del Parlamento Europeo y del Consejo, DO nº L-181, 14 de julio de 2009, que confirma la necesidad de respetar la Directiva a la hora de transmitir datos sanitarios dentro de la UE. HEREDERO HIGUERAS, "La Transmisión Internacional…", cit., 2006, p. 195.

[3051] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Lucha contra el VIH/sida en la Unión Europea y los países vecinos, 2009-2013", COM (2009) 569 final, 26 de octubre de 2009.DE MIGUEL SÁNCHEZ, *Tratamiento de datos…,* cit., 2004, p. 130.

[3052] Resolución AEPD TI/00150/2009, 26 de enero de 2010, en la que se autoriza una transferencia de datos de una empresa a una sucursal en Vietnam, en la que se incluyen datos de salud, de religión e, incluso, de orientación sexual de los trabajadores; Resolución de la AEPD TI/00052/2009, 19 de mayo de 2009.

[3053] Resolución AEPD TI/00017/2009, 11 de mayo de 2009.

[3054] Artículo 11.4 R (97) 5: *"Salvo que la ley nacional disponga otra cosa, el flujo transfronterizo de datos médicos a un Estado que no asegura la protección de acuerdo con la Convención y con esta recomendación, el flujo no debe tener lugar a menos que:*
a) se hayan tomado las medidas necesarias, incluidas aquellas de naturaleza contractual, para que se respeten los principios de la Convención y de esta recomendación, y el afectado haya tenido la posibilidad de oponerse a la transferencia".

CAPÍTULO 6. LOS DERECHOS DE LOS PACIENTES CON RESPECTO A LOS DATOS SANITARIOS QUE LES CONCIERNEN.

El presente capítulo se dedicará al análisis de los que se denominan en el Título tercero de la LOPD "Derechos de las Personas". En este apartado son varios los derechos que se reconocen: derecho a la impugnación de valoraciones, derecho de consulta al Registro General de Protección de Datos, derecho de acceso, derecho de cancelación y rectificación, derecho de oposición, derecho a la tutela de los derechos y derecho de indemnización. Todos ellos tienen gran relevancia, sin embargo, sólo se van a analizar aquí los que presentan ciertas particularidades en el ámbito sanitario. Fundamentalmente se trata de los derechos de acceso, de rectificación y cancelación, de oposición, de impugnación de valoraciones y de indemnización.

I. ASPECTOS COMUNES EN LA REGULACIÓN DE LOS DERECHOS QUE COMPONEN EL *HABEAS DATA*.

I.1. La importancia de los derechos de las personas.

La Ley reconoce en un apartado concreto los derechos arriba citados y les otorga la calificación de "derechos de las personas". A lo largo de este trabajo se han analizado diferentes elementos a los que se les ha dado la consideración de derechos. Así ha ocurrido con el consentimiento o la información, que si bien cuentan con componentes claros de derechos subjetivos son, sin embargo, reconocidos en la Ley como principios. Ya se ha visto que muchas veces la distinción entre derechos y principios no es clara. En relación a las figuras que ahora se van a analizar, derecho de acceso, cancelación, rectificación, oposición, etc., la LOPD no deja lugar a dudas sobre su consideración como derechos, lo que lleva a crear en la Ley un apartado específico dedicado a la regulación de los mismos. Parece claro el criterio que el legislador ha seguido para crear esta sección. Se basa en el hecho de que los derechos de las personas constituyen un cuerpo de facultades que cuenta con personalidad e importancia particular. Esta relevancia puede subrayarse desde diferentes puntos de vista.

Desde un punto de vista sustantivo la importancia de estos derechos deriva de la posición que ocupan en el contenido del derecho a la autodeterminación informativa[3055]. Hay que recordar que este último no es otra cosa que la facultad de controlar los datos que a uno le corresponden. Pues bien, este control se ejerce fundamentalmente mediante los derechos reconocidos en el Título III de la Ley. Los principios que se han analizado hasta ahora, incluso los derechos al consentimiento y a ser informado, constituyen criterios o directrices que han de seguir los responsables de los ficheros a la hora de llevar a cabo cualquier tratamiento. Toda manipulación de datos debe atender a las exigencias que derivan de los principios. En cambio, los derechos a los que aquí se va a hacer referencia, si bien cuentan con un vínculo muy importante con los principios, sobre todo con los principios de calidad, no son tanto directrices que han de cumplir los responsables o encargados de los ficheros, sino facultades que pueden ejercer los titulares de los datos. Se trata de derechos que éstos pueden llevar a cabo, como instrumentos de control

[3055] PUENTE, "Derechos de las personas…", cit., 2008, p. 253, señala que estos derechos constituyen uno de los elementos esenciales del derecho a la autodeterminación informativa.

sobre la información que le concierne. Como se ha visto, la autodeterminación informativa constituye, más allá de la obligación de quienes vayan a manipular la información de no realizar intromisiones ilegítimas en la esfera que cada uno quiere reservar o proteger de terceros, una facultad positiva de controlar los datos que corresponden a cada uno. Esta facultad positiva se refleja en los derechos de acceso, cancelación, rectificación, oposición, etc., que no son otra cosa que un ejercicio activo, de hacer, de los titulares del derecho[3056]. Se podría decir que parte fundamental del contenido del citado derecho a la autodeterminación informativa, el que otorga entidad propia al mismo, se compone de los derechos que se van a analizar[3057]. Se trata de facultades que dan un carácter propio al derecho a la autodeterminación informativa. Lo que se ha venido en llamar *habeas data*[3058] constituye un conjunto de derechos, que configura la posibilidad de control activo que representa el derecho fundamental reconocido en el artículo 18.4 CE[3059].

Desde un punto de vista formal la relevancia citada se reconoce expresamente en las leyes. La Exposición de Motivos de la LORTAD señalaba que "*los derechos de acceso a los datos, de rectificación y de cancelación se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley".* La propia LOPD deja entrever también esta importancia. En relación a los ficheros preexistentes a la entrada en vigor de la Ley dispone que "*En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados"*[3060]. La Ley otorgaba un plazo de adecuación a favor de los ficheros y tratamientos manuales para que pudieran adaptarse a su contenido. Sin embargo, reconocía la aplicabilidad directa de los citados derechos: los titulares de los datos podían ejercerlos durante ese periodo de adaptación. El hecho de que se hiciera referencia a estos derechos y no a otros contenidos da fe de su consideración como parte esencial del derecho fundamental a la protección de datos. Esta especial relevancia ha sido puesta de manifiesto también por la jurisprudencia[3061]. En el mismo sentido, la doctrina ha subrayado que estas facultades constituyen parte del núcleo esencial del derecho a la autodeterminación informativa, siendo los que en la práctica otorgan particularidad al mismo, de tal forma que sin ellos desaparecería[3062].

[3056] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 257.
[3057] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, pp. 325-326.
[3058] DEL PESO NAVARRO, *Ley de Protección...*, cit., 2000, p. 53: "Este derecho (el de acceso) junto a los siguientes de rectificación, cancelación y oposición son importantes pues en su conjunto delimitan lo que se puede entender como *habeas data* o *habeas scriptum*".
[3059] OROZCO PARDO, "Notas acerca del Régimen...", cit., 1998, p. 864: "Son los "elementos nutrientes" del derecho fundamental antes citado".
[3060] DA segunda LOPD.
[3061] STC 30 de noviembre del 2000, FFJJ 5 y 6, en los que se reconoce que estos derechos configuran lo que se ha venido en llamar *habeas data* o la facultad positiva de controlar los datos que a uno se refieren, dando un contenido particular al derecho a la autodeterminación informativa que lo distingue del derecho a la intimidad.
[3062] SÁNCHEZ CARAZO, *La Intimidad…,* cit., 2000, p. 160; MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...*, cit., 2001, p. 235; HERRÁN ORTIZ, *El Derecho a la Intimidad...*, cit., 2002, p. 246; SERRANO PÉREZ, *El Derecho Fundamental...*, cit., 2003, p. 184; COUDERT, Fanny, "Ejercicio de Derechos…", cit., 2007, p. 401.

La virtualidad de estos derechos va más allá de su consideración como facultades indispensables de control sobre los datos de cada uno. Su relevancia deriva también de la importancia que tienen a la hora de asegurar la calidad de la información y garantizar así, que la finalidad que se persigue con el tratamiento de datos pueda verse cumplida. En el ámbito estrictamente sanitario se ha repetido en numerosas ocasiones que es fundamental guardar la calidad de la información. No hay un buen servicio o una buena asistencia sin información de calidad. Es más, una mala información sanitaria puede llevar a tomar decisiones equivocadas que tengan efectos perjudiciales para los interesados. El adecuado ejercicio de los derechos de acceso, rectificación y cancelación constituye base necesaria para que esa calidad se mantenga en todo momento, pues garantiza que los datos reflejen la realidad exacta, veraz y actual de las personas. Rectificar la información que se estima equivocada, cancelar los datos que no sirven para conseguir la finalidad pretendida, acceder a la información obrante en los ficheros para conocer su calidad, son instrumentos necesarios para que los datos que se pretenden manipular con el objetivo de proteger la salud de las personas puedan servir a esa causa.

En conclusión, y centrándose en lo que aquí interesa, los derechos a los que ahora se hace referencia constituyen un cuerpo de facultades que guarda relevancia desde dos perspectivas. Primero, como instrumentos para ejercer el control sobre los datos de cada uno. Y segundo, como facultades cuyo ejercicio se comprende imprescindible para asegurar la calidad de la información que se vaya a manejar, para poder prestar un servicio adecuado con el fin genérico de proteger la salud de las personas.

I.2. La regulación común dada a los derechos en la normativa de protección de datos.

Destacada la especial importancia de los derechos de acceso, cancelación, rectificación, oposición, a la impugnación de valoraciones y de indemnización, conviene referirse a la regulación que de los mismos se realiza en la normativa general de protección de datos. Se trata de una cuestión que ha sido suficientemente analizada por la doctrina, por lo que sólo se acercarán ahora los aspectos más importantes.

La regulación de estos derechos en las normas resulta detallada. En el ámbito interno la LOPD y el reglamento que la desarrolla configuran, al hilo de lo que dispone la Directiva europea[3063], un marco jurídico preciso que determina el contenido de los derechos, la forma de ejercerlos, las excepciones aplicables, etc. La Ley estatal realiza una remisión al reglamento para que determine el procedimiento para ejercer estos derechos[3064]. Hasta hace unos años eran el reglamento que desarrollaba la anterior Ley de protección de datos[3065] y la Instrucción de la

[3063] Artículos 12 a 15 y 22 Directiva 95/46/CE.

[3064] Artículo 17 LOPD: "*Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, asó como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación".

[3065] RD 1332/1994, 20 de junio, por el que se desarrolla determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación el tratamiento automatizado de los datos de carácter personal.

AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación[3066], los instrumentos normativos que regulaban esta materia. Hoy día es el RDLOPD el que determina la mayoría de aspectos vinculados al ejercicio de los mismos. Esta disposición general recoge varios puntos que regulan aspectos aplicables a todos los derechos[3067].

I.2.1. La vinculación entre el derecho de acceso, de cancelación, rectificación, de oposición, de impugnación de valoraciones y de indemnización con el derecho a ser informado.

A la hora de señalar estos puntos comunes hay que comenzar subrayando su relación con el derecho de información. Si bien no se trata de una cuestión regulada en las normas, es importante mencionarla para tener presente la relevancia de la obligación de informar sobre estos derechos. La principal línea de relación la constituye el hecho evidente de que para poder llevar a cabo el acceso, la cancelación, el acceso, la oposición, etc. es necesario, en primer lugar, conocer estos derechos. Este conocimiento se lleva a cabo precisamente con el cumplimiento de la obligación de informar. Como ya se vio, las normas obligan al responsable a dar a conocer a los titulares de los datos la posibilidad y la forma de ejercer dichas facultades[3068]. En el mismo sentido, en relación a los ficheros de titularidad pública señala la Ley que en las disposiciones que crean dichos ficheros se ha de fijar la ubicación de los órganos ante quienes se pueden ejercer dichos derechos[3069]*.* La importancia de informar sobre estos puntos al titular de los datos radica en que en la práctica supone darle a conocer la forma en que puede controlar positivamente las circunstancias que rodean a la manipulación de sus datos.

La relación entre la información y estos derechos se manifiesta sobre todo cuando la obligación de informar se exceptúa. En estos casos cabe preguntarse si no se están limitando también los denominados derechos de la persona por la vía de hecho. Exceptuar la obligación de informar puede llevar a situaciones en que el titular de los datos desconozca la propia existencia de los derechos al acceso, cancelación, rectificación y oposición. En la medida en que no se facilite la información se hace difícil que los titulares de los datos conozcan la existencia y el modo de llevar a cabo el ejercicio de los derechos.

En este sentido parecen ahora acertadas las críticas que más arriba se exponían al régimen de excepciones dispuesto en la LOPD a la obligación de informar. Hay que recordar que la Ley limita el derecho a ser informado, entre otros extremos, sobre la existencia de los citados derechos, cuando este *"contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban*"[3070]. La crítica se fundamentaba en el hecho de que la excepción desemboca en una situación de desconocimiento para el titular de los datos de cómo llevar a cabo los derechos personales que le corresponden, basándose además en argumentos poco claros y sólidos. ¿Cuándo pueden deducirse los derechos de acceso, cancelación, rectificación y oposición de la naturaleza de los datos que se

[3066] Instrucción 1/1998, 19 de enero, de la AEPD, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
[3067] Artículos 23 a 26 RDLOPD.
[3068] Artículo 5.1.d) LOPD.
[3069] Artículo 20.2.g) LOPD.
[3070] Artículo 5.3 LOPD.

recogen o de las circunstancias en que se recaban? Parece difícil reconocer una situación en que se dé esta circunstancia. Además, ¿en qué bien jurídico se fundamenta esta excepción para no informar sobre la existencia de los citados derechos? Teniendo en cuenta la significación de los derechos de las personas, parece importante subrayar la necesidad de que se restrinja especialmente la aplicabilidad de esta excepción a la obligación de informar.

Por la misma razón puede resultar criticable el contenido del artículo 24 de la LOPD, que exceptúa el derecho a ser informado cuando la Administración manipula los datos y dicho tratamiento afecte a la "*defensa nacional, a la seguridad pública o a la persecución de infracciones penales*"[3071]. La ambigüedad de los términos empleados hace que el ámbito de aplicación de la excepción cuando los datos son empleados por la Administración pueda ser especialmente grande. Habida cuenta que en la práctica la excepción a la obligación de informar implica muchas veces limitar la posibilidad de ejercer los derechos personales, la amplitud de estas excepciones puede llevar a que la vigencia del derecho a la autodeterminación informativa quede especialmente restringida. En todos los casos citados, si la eliminación del derecho a la información conlleva la limitación *de facto* de los derechos de acceso, rectificación, cancelación, oposición, etc. se encontrará con que el derecho a la autodeterminación informativa queda vacío de contenido: si no se informa de la existencia del fichero, ni se facilita que se ejerzan los derechos de la persona, la facultad de controlar la información concerniente a uno mismo desaparece prácticamente[3072].

I.2.2. Identificación de los sujetos que pueden ejercer estos derechos.

Constituye un punto importante la determinación de quién puede ejercer los derechos de la persona una vez conozca la existencia de los mismos. Hoy día la regulación de este punto se lleva a cabo de manera exhaustiva en el RDLOPD. Señala la norma que los derechos deberá ejercerlos el afectado. Sin embargo, se reconoce la posibilidad de que se lleven también a cabo a través de representante en dos supuestos: cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite su ejercicio y cuando el propio afectado haya nombrado voluntariamente a un representante[3073].

De inicio, al ser los derechos de acceso, cancelación, rectificación y oposición personalísimos, deberán ser ejercidos por los propios titulares de los datos. Para ello deberán acreditar su identidad mediante el DNI o un documento equivalente[3074]. Tiene sentido fijar este punto de partida por cuanto que es el titular de los datos el que mejor conoce la información

[3071] Artículo 24.1 LOPD.

[3072] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...,* cit., 2001, p. 177: "Habilitadas determinadas Administraciones para recabar, o ceder, datos personales con el consentimiento del afectado, y en ocasiones incluso sin su conocimiento, queda a éste el remedio de ejercitar los derechos de acceso, rectificación y cancelación a fin de, respectivamente, averiguar que datos suyos posee la Administración. Así lo hacía pensar en primera instancia los artículos 13 a 16 de la Ley Orgánica, que se refieren a estos derechos. Sin embargo, fiel a su técnica, la ley estableció excepciones en otro Título".

[3073] PUENTE, "Derechos de las personas…", cit., 2008, p. 256.

[3074] Artículo 23 RDLOPD: "*1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado. 2. Tales derechos se ejercitarán: a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente*".

relativa a su persona y el principal capacitado para llevar a cabo acciones dirigidas a asegurar la buena "calidad" y el control sobre dicha información.

El reglamento se refiere en este apartado al "afectado" a la hora de hacer referencia al titular de los datos que ejercerá los derechos. Esta referencia no sigue lo señalado por la LOPD, que en relación a estos conceptos emplea tanto el término de "*afectado"* como de *"interesado*", si bien principalmente este último[3075]. El uso de uno u otro no plantea problemas prácticos pues ambos se refieren a la misma realidad. Sin embargo, cabe hacer un breve comentario sobre este hecho debido al significado teórico que tiene. La importancia del uso del concepto afectado o interesado se puso de manifiesto al comparar el contenido de la anterior Ley de protección de datos, LORTAD, con la actual, LOPD. La norma derogada recogía la misma definición que la actual Ley sobre el titular de los datos, pero se refería exclusivamente al *"afectado"*, sin emplear el término "*interesado*". La LOPD, tal y como lo hace la Directiva, utiliza mayoritariamente en su articulado el concepto de interesado, no tanto el reglamento que desarrolla la Ley, que extrañamente rompe la tendencia que había iniciado la Ley orgánica de dejar en desuso el término "afectado"[3076]. Si bien se trata de una cuestión meramente conceptual, de poco sentido práctico, la inclusión de este concepto tiene su razón de ser. El término afectado tiene cierta connotación negativa pues parece referirse al titular de los datos como persona que de alguna manera "sufre" el tratamiento de éstos. Y en este sentido, hay que traer aquí lo que ya se ha comentado: no se pueden valorar las nuevas tecnologías como un factor negativo, sino como una oportunidad[3077]. El concepto de interesado responde mejor a esta filosofía. Es por ello por lo que no se acaba de entender porqué el RDLOPD emplea en este apartado dedicado a los derechos de las personas mayoritariamente el concepto de afectado.

Más allá del propio titular de los datos, el reglamento actual reconoce la posibilidad de actuar a través de representante. La figura de la representación estaba prevista ya en normas anteriores a la entrada en vigor del RDLOPD, fundamentalmente en la Instrucción de la AEPD relativa al ejercicio de los derechos de acceso, rectificación y cancelación[3078]. Sin embargo, la normativa actual presenta una novedad lógica y necesaria con respecto a las normas anteriores. La Instrucción reconocía la posibilidad de representación. No obstante, ésta se limitaba a los casos en que el titular de los datos no pudiera ejercer los derechos por incapacidad o por ser menor de edad. El reglamento actual da un paso más y habilita al titular para que pueda nombrar un representante de manera voluntaria. Esta posibilidad ya venía prevista en la normativa vasca de

[3075] Artículo 3.e) LOPD: "*Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo".*

[3076] DEL PESO NAVARRO, *Ley de Protección...,* cit., 2000, p. 15, afirma que "parece que existía cierto pudor al empleo de la palabra pero no ha sido suficiente para haberla eliminado".

[3077] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 35.

[3078] Norma segunda Instrucción 1/1998, de 19 de enero, de la APD, relativa al ejercicio de los Derechos de Acceso, Rectificación y Cancelación, BOE nº 25, 29 de enero de 1998: "*Requisitos generales.- 1. Los derechos de acceso a los ficheros automatizados, así como los de rectificación y cancelación de datos son personalísimos y serán ejercidos por el afectado frente al responsable del fichero por lo que será necesario que el afectado acredite su identidad frente a dicho responsable. Estos derechos se ejercerán sin otras limitaciones que las que prevén la Ley Orgánica 5/1992 y el Real Decreto 1332/1994, de 20 de junio.*

Podrá, no obstante, actuar el representante legal del afectado cuando éste se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de los mismos, en cuyo caso será necesario que el representante legal acredite tal condición".

protección de datos[3079] y la AEPD ya se había hecho eco también, en alguno de sus informes posteriores a la citada Instrucción, de la necesidad de extender la figura de la representación a los supuestos en que así lo deseara el titular de los datos[3080].

En definitiva, la representación puede darse en diferentes supuestos. A) En primer lugar, cuando el titular de los datos se encuentre en situación de incapacidad o minoría de edad que imposibilite el ejercicio personal de dichos derechos, los llevará a cabo el representante legal que acredite dicha condición[3081]. En estos casos, el responsable del fichero deberá cerciorarse de la condición de menor o incapaz del titular de los datos y de la veracidad de la condición de representante de quien ejercerá los derechos de parte del titular[3082]. A la hora de verificar dichas circunstancias el nivel de exigencia en el esfuerzo que el responsable del fichero debe realizar no puede ser desproporcionado. Como señala la doctrina, esta exigencia no va más allá de la comprobación de que se dan la minoría de edad o incapacidad y la condición de representante habilitado[3083].

Las normas vienen a decir que en el caso de los incapacitados y menores serán sus representantes quienes ejerzan los derechos. Sin embargo, en las disposiciones citadas se añade que la representación se dará cuando la incapacidad o la minoría de edad imposibilite el ejercicio personal de los derechos. El ordenamiento parece abrir una puerta para que los propios titulares ejerzan los derechos cuando les sea posible. Se plantea, por lo tanto, inevitablemente, la cuestión de si el menor, y de la misma forma el incapacitado, pueden ejercer por sí mismos los derechos a los que se está haciendo referencia. La normativa no aclara este punto por lo que es necesario realizar un ejercicio de interpretación al respecto.

El RDLOPD reconoce la posibilidad de los mayores de 14 años de consentir por sí mismos un tratamiento de datos[3084]. Partiendo de esta regulación, normas internas de determinados sistemas sanitarios han reconocido la aplicabilidad de este límite de edad, señalando que a partir de 14 años el paciente goza de las condiciones de discernimiento y madurez suficientes para realizar por sí mismo actos en la vida civil[3085]. En el ámbito sanitario la LBAP reconoce la

[3079] Artículo 4.2 Decreto 308/2005, de la Comunidad Autónoma del País Vasco, de 18 de octubre, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos: "*Para el ejercicio de los derechos a que se refiere este artículo, por medio de representante voluntario, deberá acreditarse la representación, para cada actuación concreta, por cualquier medio válido en derecho que deje constancia fidedigna o mediante declaración en comparecencia personal del interesado ante el responsable del fichero".*

[3080] Informe jurídico de la AEPD *"*Ejercicio de los Derechos de Acceso, Rectificación y Cancelación por medio de Representante", 1999: Ha estimado la AEPD que "de lo dispuesto en el artículo 11 del Real Decreto 1332/1994 no se desprende una prohibición del ejercicio de los derechos de acceso, rectificación y cancelación por un representante voluntario o mandatario del propio afectado, considerándose el ejercicio del derecho por el mandatario como efectuado por el propio interesado que le confiere la representación".

[3081] Artículo 23.2.b) RLOPD.

[3082] COUDERT, "Ejercicio de Derechos…", cit., 2007, p. 402.

[3083] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 262.

[3084] Artículo 13 RDLOPD: "*Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores*".

[3085] Artículo 4.3.1 Resolución de 27/02/2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam.

posibilidad de que menores no incapaces ni incapacitados, pero emancipados o con dieciséis años cumplidos, otorguen el consentimiento sin representación, en este caso, para recibir asistencia sanitaria[3086]. Con respecto al derecho a recibir información señala esta Ley que el paciente será informado en todo caso atendiendo a sus posibilidades de comprensión, incluso en los supuestos de incapacidad[3087]. La normativa sanitaria autonómica lleva a cabo una regulación semejante, si bien en algunos casos se otorga también a los mayores de doce años cierta capacidad a la hora de consentir una intervención clínica[3088]. La normativa general dirigida a proteger los derechos de los menores de edad parece ir más allá y atiende más al criterio de la madurez, sin fijar regulaciones definidas en base a edades predeterminadas. El código civil abre la puerta para que dependiendo de la madurez del menor, incluso del menor de 16 o 14 años, éste pueda llevar a cabo los derechos que se comentan por sí mismo[3089]. Así lo hace también la normativa dirigida a proteger en el ámbito civil los derechos de honor, intimidad e imagen[3090], y lo mismo podría deducirse de la normativa dirigida a proteger, en general, los derechos del menor[3091]. Los tribunales también han parecido adoptar una postura cercana a esta previsión, reconociendo que los menores tienen plena capacidad para disfrutar de sus derechos sin que su ejercicio pueda abandonarse por completo a los representantes de dichos menores[3092]. También la doctrina ha reconocido que el criterio de madurez será el que deba tenerse en cuenta en el caso de los menores, a la hora de determinar si tienen la capacidad de ejercer los derechos por sí mismos[3093]. La misma línea interpretativa se ha seguido desde el Grupo de Trabajo del artículo 29 de la Directiva europea sobre protección de datos[3094]

[3086] Artículo 9.3 LBAP.
[3087] Artículo 5.2 LBAP.
[3088] Artículo 43.2 Ley Foral 17/2010, 8 de noviembre, de Derechos y Deberes de las Personas en materia de Salud en la Comunidad Foral de Navarra: "*También serán titulares del derecho a la información sobre la salud del menor sus padres o tutores cuando aquél sea menor de dieciséis años si deben prestar el consentimiento informado en su nombre, sin perjuicio del derecho del menor a recibir información sobre su salud en un lenguaje adecuado a su edad, madurez y estado psicológico*"; Artículo 7.3 Ley 1/2003, 28 de enero, de Derechos e Información al Paciente de la Comunidad Valenciana: "*En el caso de menores, se les dará información adaptada a su grado de madurez y, en todo caso, a los mayores de doce años. También deberá informarse plenamente a los padres o tutores que podrán estar presentes durante el acto informativo a los menores. Los menores emancipados y los mayores de dieciséis años son titulares del derecho a la información*".
[3089] Artículo 162 CC: "*Los padres que ostentan la patria potestad tienen la representación legal de sus hijos menores no emancipados. Se exceptúan: 1. Los actos relativos a derechos de la personalidad u otros que el hijo, de acuerdo con las leyes y con sus condiciones de madurez, pueda realizar por sí mismo (...)*". DE LORENZO Y MONTERO y ESCUDERO GONZÁLEZ, "El derecho de acceso…", cit., 2010, p. 1.206, cita un importante número de normas autonómicas que disponen una regulación variada a este respecto, lo cuál dificulta la adopción de un criterio único sobre cuándo un menor puede acceder a su historia clínica.
[3090] Artículo 3.1 LO 1/1982, 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia Imagen: "*El consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil*".
[3091] Artículo 5.1 LO 1/1996, 15 de enero, de Protección Jurídica del Menor: "*Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo*"
[3092] STC 18 de julio de 2002 FJ 10.
[3093] BENAC URROZ, "La Problemática del Menor…", cit., 2004, p. 79 y siguientes: sobre el menor maduro y la posibilidad de que sea él quien lleve a cabo los derechos de acceso, etc; ABEL LLUCH, "El derecho de información…", cit., 2004, p. 45 y siguientes, en el mismo sentido.
[3094] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 96/46/CE, 1/2008, sobre la protección de datos de carácter personal de los niños, 18 de febrero de 2008 y Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2009, sobre la protección de los datos personales de los niños, 11 de febrero de 2009.

Esta regulación parece otorgar mayor capacidad de obrar de la que en un inicio podría deducirse del RDLOPD a los menores de edad[3095]. Parece lógico aceptar que si cuando se trata de consentir un tratamiento de datos o una intervención médica a determinados menores se otorga dicha capacidad, también la tendrán en el caso del ejercicio del derecho al acceso, cancelación, rectificación u oposición, en la medida en que se trata de situaciones de menor riesgo para los interesados[3096]. La normativa parece dar margen para que se adopte un criterio relativamente amplio a la hora de otorgar capacidad de obrar al menor[3097].

Resulta relevante otorgar esta capacidad de control a los menores sobre sus datos en un sector como el sanitario, donde se manipula información que puede resultar de especial sensibilidad. La necesidad de fortalecer la autonomía del menor lleva a tomar esta posición. Hay que tener en cuenta que pueden encontrarse casos en que, por ejemplo, el menor no quiere que sus representantes conozcan determinada información sobre su estado de salud o sobre aspectos que inciden en ésta[3098]. O supuestos en que tenga una posición distinta a la de sus representantes a la hora de ejercer sus derechos. Estos argumentos justifican la necesidad de adoptar un criterio en que los menores e incapaces puedan tener la posibilidad de ejercer los derechos por sí mismos.

Se entiende aquí que dependiendo principalmente de la madurez del sujeto, que deberá ser valorada por el profesional que le trata, se determinará si este titular de los datos puede ejercer por sí mismo los derechos. La valoración del profesional deberá tener en cuenta el contenido de la información sobre la que se quiere ejercer el derecho, la influencia que dicho ejercicio pueda tener sobre la salud del menor, la capacidad que éste pueda tener para comprender estas circunstancias o si es necesario que los representantes conozcan los datos para mejorar el tratamiento.

B) En segundo lugar, los casos de representación pueden ir más allá de los que afectan a menores de edad e incapaces. A pesar de haber sido una cuestión debatida en sede judicial[3099], la representación puede ser voluntaria, según el RDLOPD. Estos derechos pueden ser ejercidos por un representante voluntariamente elegido por el titular de los datos. Esta representación

[3095] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 247.

[3096] "El Menor Maduro tiene Derecho a acceder a su Historia Clínica", *Diariomédico.com,* 7 febrero 2005, en http://www.diariomedico.com, recoge la opinión a este respecto de Antonio TRONCOSO, que se manifiesta en el mismo sentido que en expuesto.

[3097] MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 55; GÓMEZ PIQUERAS, "La historia clínica…", cit., 2009, p. 149; ARENAS RAMIRO, "El derecho de acceso…", cit., 2010, p. 1.171.

[3098] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 1/2008, sobre la protección de datos de carácter personal de los niños, 18 de febrero de 2008 y Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 2/2009, sobre la protección de los datos personales de los niños, 11 de febrero de 2009. DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 592; PÉREZ LUÑO, "El consentimiento de los menores…", cit., 2010, p. 488; TRONCOSO REIGADA, *La Protección de Datos...*, cit., 2010, p. 1.232.

[3099] STS 15 de julio de 2010, FJ 11, en la que se cuestionaba la validez de la representación voluntaria prevista en el RDLOPD. Acaba señalando el TS que, a pesar de tratarse de una posibilidad no prevista en la LOPD, la representación voluntaria es acorde a Derecho, en la medida en que se reconocen en el ordenamiento otra serie de supuestos en que derechos personalísimos pueden ser ejercidos por representante, caso del matrimonio. La STEDH 28 de abril de 2009, K. H. and Others v. Slovakia, FFJJ 44-58, analiza el supuesto en que los abogados de unas personas a las que se causó una lesión en un centro sanitario quieren acceder a las historias clínicas de sus clientes y hacer fotocopias de las mismas, con su autorización, y acaba reconociendo esta posibilidad.

constituye una alternativa para llevar a cabo ejercicios puntuales de los derechos. En ningún momento puede convertirse en una delegación de facultades, sino que se tratará de que el representante actúe dentro de los parámetros concretos marcados por el titular de los datos en un momento determinado[3100].

Para ejercer esta representación la normativa exige acreditación de la identidad del representado, a través de la copia del DNI o documento equivalente, y la representación conferida por el titular de los datos[3101]. En los casos en que los derechos se ejercen a través de representante y el responsable del fichero es una Administración, la representación podrá acreditarse por cualquier medio que deje constancia fidedigna de dicha representación o mediante declaración en comparecencia personal del interesado[3102]. La norma exige que el representante cuente con un apoderamiento especial para ejercer la representación[3103]. Sin embargo, en principio, parece dejarse la puerta abierta para que sea cualquiera la forma de acreditar la representación, pues no se señala ninguna vía concreta. En este sentido, en el ámbito privado el CC no exige la forma escrita para formalizar el mandato, que es la figura más cercana a este tipo de acto de representación[3104]. En el ámbito de la Administración, el citado precepto del reglamento viene a reproducir lo que ya dictaba la LPAC[3105]. Sea como sea, parece lógico pensar que la fórmula más corriente de acreditar la representación será la escrita. Así, en algún momento la AEPD ha llegado a exigir que el mandato se lleve a cabo de forma escrita con el fin de que el responsable del fichero ante el que se ejerce el derecho pertinente tenga conocimiento claro, directo y expreso de la voluntad del titular de los datos[3106]. Sea mediante la fórmula escrita u otra que asegure la acreditación de la representación, el responsable del fichero ante quien se ejercen los derechos deberá verificar que el representante voluntario presenta el poder otorgado por el titular de los datos[3107].

[3100] Informe jurídico AEPD, "Ejercicio de los Derechos de Acceso, Rectificación y Cancelación por medio de Representante", 1999.

[3101] Artículo 23.2.c) RDLOPD: "*Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberán constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél*".

[3102] Artículo 23 RDLOPD: "*c) Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de las Administraciones de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.*

[3103] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 262, p. 263.

[3104] Artículo 1709 CC: "*Por el contrato de mandato se obliga una persona a prestar algún servicio o hacer alguna cosa, por cuenta o encargo de otra*", artículo 1710 CC: "*El mandato puede ser expreso o tácito; el expreso puede darse por instrumento público o privado y aun de palabra; la aceptación puede ser también expresa o tácita, deducida esta última de los actos del mandatario*".

[3105] Artículo 32 LPAC: "*2. Cualquier persona con capacidad de obrar podrá actuar en representación de otra ante las Administraciones Públicas. 3. Para formular solicitudes, entablar recursos, desistir de accesiones y renunciar a derechos en nombre de otra persona, deberá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado. Para los actos y gestiones de mero trámite se presumirá aquélla representación*". SÁNCHEZ MORÓN, *Derecho Administrativo…,* cit., 2007, p. 482.

[3106] Informe jurídico AEPD, "Ejercicio de los Derechos de Acceso, Rectificación y Cancelación por medio de Representante", 1999. PUENTE, "Derechos de las personas…", cit., 2008, p. 261.

[3107] COUDERT, Fanny, "Ejercicio de Derechos…", cit., 2007, p. 403.

Se han citado los sujetos que pueden llevar a cabo los derechos de la persona. Así, sólo pueden ejercerse mediante el propio interesado o, en diferentes supuestos, a través de representante. En todo caso, deberá acreditarse que estas vías se emplean cumpliendo con los requisitos arriba citados. Esta acreditación se realizará en la solicitud que el titular o el representante presentará ante el responsable del fichero. Si en dicha solicitud hay algún error en relación a la acreditación de la representación o cualidad del interesado, el titular de los datos tendrá la posibilidad de subsanar el error o vicio. Si bien es cierto que el reglamento no fija esta posibilidad de subsanación expresamente para estos casos, esta alternativa se deriva de la regulación general del procedimiento, que sí la reconoce para los defectos de la solicitud en general[3108]. Si no se produce subsanación alguna o la solicitud de ejercicio de estos derechos se quiere llevar a cabo a través de fórmulas diferentes a las comentadas, dicha solicitud será rechazada[3109]. Es lógica esta regulación de negar el ejercicio de los derechos en estos supuestos, por cuanto que lo contrario daría lugar a que personas sin acreditación pudieran acceder a aspectos íntimos de los titulares de los datos y manipular dicha información de modo contrario a lo dispuesto por las normas.

I.2.3. Aspectos comunes sobre cómo ejercer estos derechos.

El ejercicio de estos derechos no presenta mayores complicaciones en la medida en que la normativa fija detalladamente el procedimiento que se ha de seguir para ello. El reglamento actual, atendiendo a lo que disponía antes la Instrucción de la AEPD de 1998[3110], determina los pasos a seguir para la realización de los derechos[3111].

En primer lugar, se refuerza el principio de sencillez en el procedimiento[3112]. Este principio, en lo tocante al ejercicio de los derechos ante administraciones públicas, ya venía reconocido implícitamente en la LPAC por los principios de celeridad[3113] e impulsión de oficio[3114]. Sin embargo, el RDLOPD lo generaliza para todos los supuestos en que se quieran llevar a cabo estos derechos. El reglamento trata de facilitar su ejercicio por diferentes medios: a) señala que deberá determinarse una vía sencilla para ello. El responsable tendrá que crear un mecanismo en el que se identifique sin problema el sistema que los interesados han de emplear para ejercer sus derechos; b) propone una vía preferente, sobre todo cuando el responsable es una organización compleja, dirigida a identificar el órgano ante el que los titulares de los datos

[3108] Artículo 25.3 RDLOPD. PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, pp. 264 y 272; PUENTE, "Derechos de las personas…", cit., 2008, pp. 275-277.
[3109] Artículo 23 RDLOPD: "*3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél*".
[3110] Norma primera de la Instrucción 1/1998, 19 de enero, de la AEPD.
[3111] Artículos 24 a 26 RDLOPD
[3112] Artículo 24.2 RDLOPD. PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 266; CARDONA RUBERT, "Derechos de acceso…", cit., 2009, p. 204.
[3113] Artículo 74.1 LPAC: "*El procedimiento, sometido al criterio de celeridad, se impulsará de oficio en todos sus trámites*".
[3114] Artículo 41.1 LPAC: "*Los titulares de las unidades administrativas y el personal al servicio de las Administraciones Públicas que tuviesen a su cargo la resolución o el despacho de los asuntos, serán responsables directos de su tramitación y adoptarán las medidas oportunas para remover los obstáculos que impidan, dificulten o retrasen el ejercicio pleno de los derechos de los interesados o el respeto a sus intereses legítimos, disponiendo lo necesario para evitar y eliminar toda anormalidad en la tramitación de procedimientos*".

pueden llevar a cabo sus derechos. Se trata de los servicios de atención al cliente[3115]. Se sugiere en la norma que estos servicios constituyen una vía adecuada para tramitar el ejercicio de los derechos[3116]; c) a pesar de proponer una vía, dispone que el titular de los datos podrá emplear otro medio, incluso distinto al preestablecido por el responsable del fichero[3117]. En este sentido, alguna resolución de la AEPD ha admitido que, cuando se trata de organizaciones complejas, los derechos pueden llevarse a cabo fuera de los sitios dispuestos para ello, por ejemplo, en sucursales o departamentos de dichas organizaciones[3118].

En segundo lugar, el RDLOPD subraya la gratuidad del procedimiento[3119]. Se trata de evitar procedimientos costosos para los interesados y, sobre todo, que el responsable configure en el ejercicio de estos derechos una vía para lucrarse a cuenta de los titulares de los datos[3120].

En tercer lugar, recoge un procedimiento concreto para ejercerlos, si bien reconoce que este procedimiento general puede alterarse si así lo determinan otras normas[3121] o lo exigen motivos de seguridad pública[3122]. Los aspectos principales de dicho procedimiento no presentan mayor complicación. Deberá presentarse una solicitud concretando diferentes aspectos sobre la identificación del titular de los datos, la petición que se realiza, la dirección a efectos de notificación, y aportando, en su caso, documentación que acredite dicha petición[3123]. Si la solicitud cuenta con algún defecto el responsable deberá exigir su subsanación[3124]. No se señala

[3115] Artículo 24.4 RDLOPD. PUYOL MONTERO, "Los derechos de acceso", cit., 2008, p. 268.

[3116] Artículo 5.1 Resolución de 27/02/2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam, señala el Servicio de Atención al Usuario como órgano preferente para tramitar las solicitudes de cancelación, rectificación, acceso u oposición.

[3117] Artículo 24.5 RDLOPD: "*El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente*".

[3118] Resolución de la AEPD R/01127/2009, 27 de abril de 2009, procedimiento TD/01640/2008: En este caso el titular ejerce el derecho de acceso frente a Telefónica, pero no lo hace dirigiéndose a la central o al departamento expresamente establecido para ello. Aún así, la AEPD señala que "la solicitud por cualquier departamento o sucursal del responsable es destino válido de la misma". Resolución APDCM, 28 de septiembre de 2009, "El derecho de acceso a los datos personales no puede ser limitado por el responsable obligando a la utilización de determinados modelos y procedimientos", en la que se señala que a pesar de que el responsable del fichero haya fijado una vía concreta para llevar a cabo el derecho de acceso, el que el titular de los atos no haya utilizado esta vía no hace que dicho responsable no tenga la obligación de satisfacer el acceso.

[3119] Artículo 24.3 LOPD: "*El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.*

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado".

[3120] FERNÁNDEZ LÓPEZ, "Algunas reflexiones…", cit., 2007, p. 58, señala que el hecho de que el ejercicio de los derechos sea gratuito puede limitar las fórmulas para llevarlos a cabo; PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, pp. 266-267.

[3121] Articulo 25.8 RDLOPD.

[3122] Artículo 25.7 RDLOPD.

[3123] Artículo 25.1 RDLOPD.

[3124] Artículo 25.3 RDLOPD.

plazo alguno para poder presentar las correcciones, sin embargo, parece evidente que hasta que éstas no se lleven a cabo no se podrá tramitar la solicitud. El responsable estará obligado a contestar la solicitud presentada por el titular de los datos. Esta obligación perdura independientemente de si cuenta con datos referentes al titular o no[3125]. En caso de duda corresponderá al responsable del fichero probar que contestó a la solicitud[3126]. Cuando se trate de ficheros públicos la contestación al titular de los datos deberá de hacerse de acuerdo a las reglas de notificación dispuestas en la LPAC[3127]. Cuando los derechos se ejercen ante un encargado de fichero éste deberá trasladar la solicitud al responsable para que lo haga efectivo. El encargado podrá contestar a la solicitud por sí mismo cuando así se disponga en el contrato entre el responsable y encargado[3128].

El procedimiento descrito es común para todos los derechos. En principio, no plantea mayores problemas interpretativos, sin embargo, la jurisprudencia ha establecido matices importantes sobre la forma de realizar las solicitudes. Concretamente, ha subrayado la necesidad de que el afectado facilite por su parte lo máximo al responsable la realización de su trabajo, indicando con la mayor precisión posible a qué fichero quiere acceder, o qué datos quiere rectificar o cancelar[3129]. En algunas decisiones de la AEPD también se ha reconocido que el ejercicio de dichos derechos no puede someter al responsable a un esfuerzo desproporcionado[3130]. Cuando las solicitudes se presentan ante organizaciones que cuentan con grandes bases de datos, como puede ser un sistema sanitario, pueden presentarse complicaciones prácticas si no se especifican por parte del titular los datos sobre los que se quieren llevar a cabo los derechos. Se entiende lógica esta apreciación para facilitar su ejercicio. Sin embargo, hay que ser conscientes de que en la práctica, en muchas ocasiones, el titular de los datos desconocerá los ficheros con los que cuenta el responsable, por lo que no le será fácil concretar sobre qué fichero quiere realizar el derecho correspondiente. Atendiendo a esta

[3125] Artículos 24.5 y 25.2 RDLOPD.

[3126] Artículo 25.5 RDLOPD. BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 331. Resolución AEPD R/00711/2004, 30 de diciembre de 2004, procedimiento PS/00145/2004: corresponde al responsable del fichero probar que ha cumplido las solicitudes de acceso, cancelación, etc. del interesado y que ha notificado de dicha circunstancia al titular de los datos. SAN 3 de marzo de 2004, FJ 2: se deduce la importancia para el responsable de poder demostrar que efectivamente llevó a cabo el bloqueo de los datos dentro del plazo fijado por Ley y notificado al titular de los datos. en este caso el responsable parece poder demostrar que el bloqueo se produjo en un momento, pero no puede asegurar ni aclarar que dicho bloqueo se produjera en plazo.

[3127] Artículo 59.2 LPAC: "*En los procedimientos iniciados a solicitud del interesado, la notificación se practicará en el lugar que éste haya señalado a tal efecto en la solicitud. Cuando ello no fuera posible, en cualquier lugar adecuado a tal fin, y por cualquier medio conforme a lo dispuesto en el apartado 1 de este artículo.*
Cuando la notificación se practique en el domicilio del interesado, de no hallarse presente éste en el momento de entregarse la notificación podrá hacerse cargo de la misma cualquier persona que se encuentre en el domicilio y haga constar su identidad. Si nadie pudiera hacerse cargo de la notificación, se hará constar esta circunstancia en el expediente, junto con el día y la hora en que se intentó la notificación, intento que se repetirá por una sola vez y en una hora distinta dentro de los tres días siguientes". Resolución APDCM, 24 de septiembre de 2009, "La satisfacción por correo postal de un derecho de acceso se rige por la doble notificación prevista en el artículo 59.2 de la Ley 30/1992".

[3128] Artículo 26 RDLOPD.

[3129] SAN 21 de abril de 2004, FJ 2: "para que el acceso sea posible es necesario que el afectado realice una petición que permita al responsable del fichero la búsqueda de tales datos. Siendo lo esencial no tanto la identificación concreta del fichero como la facilitación de los datos precisos para su búsqueda".

[3130] Informes jurídicos AEPD 0296/2008 y 0381/2008: en el que se subraya la necesidad de que el interesado facilite la localización de los datos que pretende cancelar. Si no se aporta por el interesado la información necesaria para poder llevar a cabo dicha localización sin necesidad de esfuerzos desproporcionados podría denegarse la cancelación.

circunstancia, acaba apuntando la jurisprudencia que esta exigencia de concreción que se le solicita al titular de los datos para facilitar la labor del responsable ha de matizarse o relativizarse dependiendo del caso[3131].

El ejercicio de estos derechos puede hacerse también de manera remota. Hay que realizar un breve apunte sobre esta cuestión, pues este sistema es aplicable también en el ámbito sanitario en la medida en que se va generalizando la historia clínica electrónica en los distintos sistemas sanitarios. La LAE reconoce el derecho de los ciudadanos a relacionarse con las administraciones utilizando medios electrónicos y a obtener copias de los documentos electrónicos que formen parte de procedimientos en los que el titular de los datos tenga la condición de interesado[3132]. Por otro lado, la norma obliga a la Administración a poner los medios oportunos para poder hacer efectivos estos derechos[3133]. En relación a esta cuestión, el RDLOPD también se refiere a los procedimientos iniciados por medios electrónicos[3134], por lo que el procedimiento que se acaba de exponer sería aplicable también al ejercicio telemático de los derechos. En caso de laguna parece que será de aplicación lo que dispone la LAE al respecto[3135]. El ejercicio remoto del acceso, cancelación o rectificación plantea, sin embargo, ciertos problemas. Primero, es necesario que se asegure que la transmisión se va a realizar de manera segura y, sobre todo, garantizando la acreditación de la identidad del interesado[3136]. Segundo, en relación al ámbito estrictamente sanitario, el acceso remoto plantea el problema de que en un sector tan técnico o científico como el sanitario, el usuario no pueda entender la información o no encuentre asistencia de los profesionales, que como se verá constituye una máxima importante en el ejercicio de los derechos en este sector.

I.2.4. Límites comunes a los derechos de las personas.

Diferentes normas recogen una serie de supuestos comunes en que los derechos que se analizan pueden verse limitados, es decir, casos en que no pueden ser ejercidos. La LOPD, siguiendo lo que disponían anteriormente la Directiva europea[3137] y el Convenio del Consejo de

[3131] SAN 21 de abril de 2004, FJ 2: se refiere al caso en que el interesado solicita el acceso pero no concreta los ficheros a los que quiere acceder. Señala el tribunal acertadamente que en la mayoría de casos el interesado desconoce los ficheros de los que dispone el responsable (piénsese en ficheros de publicidad) y los datos con los que cuenta. Por ello, la precisión exigible al interesado en el ejercicio del acceso es muy relativa. En principio, el interesado debe especificar hasta donde sabe: cómo sabe que el responsable tiene sus datos…

[3132] Artículo 6 LAE.

[3133] Disposición Final Tercera.

[3134] Artículo 25 RDLOPD.

[3135] Artículo 35 LAE.

[3136] Artículos 14 y 15 LAE. Y artículo 4.f) LAE.

[3137] Artículo 13 Directiva: "*Excepciones y limitaciones:*
1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguarda de:
a) la seguridad del Estado; b) la defensa; c)la seguridad pública; d)la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e)un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas.

Europa de 1981[3138], señala en relación a los ficheros de titularidad pública, que no podrán ejercerse dichos derechos cuando de esa actuación pudieran derivar peligros para "*la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que estén realizando*". Como contrapunto a estas excepciones la Ley reconoce a favor del interesado la posibilidad de acudir, si se le deniega el ejercicio de alguno de los derechos, al Director de la agencia de protección de datos correspondiente para que este órgano se asegure de que el rechazo del responsable del fichero es acorde a Derecho[3139]. La Directiva recoge una excepción, que si bien tenía sitio en el Convenio de 1981, no ha sido acogida como tal en la LOPD: "*Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12*

2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadística". Considerando 43 Directiva: "*Considerando que los Estados miembros podrán imponer restricciones a los derechos de acceso e información y a determinadas obligaciones del responsable del tratamiento, en la medida en que sean estrictamente necesarias para, por ejemplo, salvaguardar la seguridad del Estado, la defensa, la seguridad pública, los intereses económicos o financieros importantes de un Estado miembro o de la Unión, así como para realizar investigaciones y entablar procedimientos penales y perseguir violaciones de normas deontológicas en las profesiones reguladas; que conviene enumerar, a efectos de excepciones y limitaciones, las tareas de control, inspección o reglamentación necesarias en los tres últimos sectores mencionados relativos a la seguridad pública, los intereses económicos o financieros y la represión penal; que esta enumeración de tareas relativas a los tres sectores citados no afecta a la legitimidad de las excepciones y restricciones establecidas por razones de seguridad del Estado o de defensa".*

[3138] Artículo 9 Convenio 108/1981 del Consejo de Europa: "*1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los limites que se definen en el presente artículo;*

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la parte, constituya una medida necesaria en una sociedad democrática: a)Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b)para la protección de la persona concernida y de los derechos y libertades de otras personas.

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentados a la vida privada de las personas concernidas".

[3139] Artículo 23 LOPD: *"Excepciones a los derechos de acceso, rectificación y cancelación.-1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que estén realizando.*

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación".

cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadística".

A) En relación a las excepciones reconocidas en la Ley estatal cabe realizar alguna crítica. En primer lugar, todas estas excepciones se recogen en la LOPD con el rango de Ley ordinaria[3140], lo que ha sido cuestionado por la doctrina[3141]. Como se ha comentado en relación a otros aspectos que también han sido regulados con este rango normativo, la consideración de la LOPD no es afortunada. La fijación de estas excepciones afecta directamente al núcleo mismo del derecho fundamental que aquí se trata. Ya se ha dicho que los derechos de acceso, cancelación, rectificación u oposición configuran un cuerpo de facultades esencial que otorga personalidad propia al derecho a la autodeterminación informativa. De esta circunstancia se puede concluir que las limitaciones a dichas facultades debían establecerse, cuando menos de inicio, a través de leyes orgánicas. No hay que olvidar que la CE exige que el desarrollo de los derechos fundamentales se lleve a cabo a través de este tipo de leyes.

En segundo lugar, cabe criticar la amplitud de los conceptos con los que se reconocen las excepciones[3142]. Las referencias a la defensa nacional, la seguridad pública, los derechos y libertades de terceros y del propio interesado, y las investigaciones constituyen conceptos especialmente amplios, que dificultan la determinación de los casos en que se pueden limitar estos derechos. Se genera así el riesgo de que se abra la puerta a que cuando son las administraciones, fundamentalmente las Fuerzas y Cuerpos de Seguridad, las que manipulan la información, los derechos queden prácticamente anulados. La referencia a la protección de los derechos y libertades de terceros resulta de especial ambigüedad, abriendo la puerta a que en la ponderación entre los intereses en juego se cree un amplio margen de actuación para negar el ejercicio de estas facultades. Señala la Ley que la realización de investigaciones también puede llevar a limitar los derechos personales. No resulta fácil determinar a qué tipo de investigación se refiere la norma en este momento. En todo caso, atendiendo a que el precepto se refiere a conceptos vinculados, en general, a la seguridad o la defensa, y a que en el artículo de la LOPD que recoge estos límites se hace remisión a las disposiciones anteriores que se refieren a los ficheros policiales, parece que se está refiriendo a investigaciones de carácter penal y no tanto a investigaciones científicas[3143].

El principal problema, se entiende aquí, reside en el hecho de que se le otorga al responsable del fichero una amplísima facultad para decidir sobre la limitación de los derechos. El empleo de conceptos tan laxos como los citados hace que el responsable disponga de un amplio margen de actuación. La Ley reconoce la posibilidad de acudir a la AEPD cuando el responsable alega cualquiera de estos supuestos para limitar el ejercicio de los derechos por el titular de los datos. Sin embargo, dispone simplemente que el titular podrá poner en conocimiento del Director de la Agencia. Ciertamente, esta facultad de "poner en conocimiento" no parece que ofrezca garantías

[3140] Disposición Final Segunda LOPD.
[3141] COLLADO GARCÍA-LAJARA, *Protección de Datos...*, cit., 2000, pp. 60-61.
[3142] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 257.
[3143] FERNÁNDEZ GARCÍA, "Artículo 23. Excepciones…", cit., 2008, p. 449.

suficientes a los ciudadanos ante la posible denegación del derecho por parte del responsable del fichero[3144]. La Agencia correspondiente deberá asegurarse de la procedencia o no de la denegación. Podría pensarse que la actuación del órgano garante del derecho a la autodeterminación informativa se acaba aquí, pero hay que abogar por exigir que la actuación de esta institución no acabe en la mera determinación de la procedencia o improcedencia de la denegación, sino que continúe con una actuación inspectora y en su caso sancionadora[3145].

B) En relación a las investigaciones, la Directiva europea plantea también otro supuesto que justifica la excepción más allá de la referencia que se acaba de hacer en la LOPD. La norma europea señala que se pueden limitar los derechos cuando no esté en juego la intimidad de los titulares de los datos, y la información se emplee con la finalidad de realizar investigaciones científicas o tenga que conservarse para realizar estadísticas. No se entiende aquí el sentido de esta limitación, que además en el ámbito interno no se ha recogido de manera expresa. En principio, parece otorgarse a los estados la posibilidad de exceptuar el ejercicio de los derechos cuando la finalidad del tratamiento de los datos es la investigación científica o la elaboración de estadísticas, siempre que se garantice que no se afecta a la "intimidad" de manera manifiesta. Sin embargo, cabe preguntarse si por intimidad se refiere a los datos sensibles y si la excepción se aplica cualquiera que sea la investigación o la estadística a realizar. Evidentemente, las investigaciones pueden tener las más diferentes finalidades. No parece adecuado que cualquiera que sea el fin pueda constituir base suficiente para limitar los derechos. Parece necesario que la investigación concreta afecte a un interés especialmente relevante.

C) La LOPD se hacía eco de otro supuesto de limitación, siguiendo lo que disponía la LORTAD[3146]. Señalaba la Ley que en aplicación del principio de proporcionalidad dichos derechos deberían verse exceptuados a favor de un interés público o de intereses de terceros más dignos de protección[3147]. Esta previsión fue declarada inconstitucional debido, fundamentalmente, a la indeterminación de sus términos[3148]. Y es que, si bien es cierto que intereses del propio afectado o de una tercera persona pueden llevar a excepcionar estos derechos, lo que no resulta aceptable es que las excepciones se fijen con tal grado de indeterminación, que dejen al responsable del fichero, que tiene que atender la ejecución de los mismos, tan amplio margen de discrecionalidad. No obstante, parte de la doctrina ha aceptado, basándose en la normativa ya derogada, que el derecho a la cancelación puede verse limitado a favor de intereses legítimos terceros o del propio afectado[3149].

[3144] HERRÁN ORTIZ, *El Derecho a la protección...*, cit., 2003, p. 81.
[3145] MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información...*, cit., 2001, pp. 181-182; FERNÁNDEZ GARCÍA, "Artículo 23. Excepciones…", cit., 2008, p. 451.
[3146] Artículo 15.4 LORTAD: "*la cancelación no procederá cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros o cuando existiese una obligación de conservar los datos"*.
[3147] Artículo 24 LOPD.
[3148] STC, 30 noviembre de 2000, FJ. 18.
[3149] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 316: antes se señalaba que se puede denegar la cancelación cuando pudiese causar un perjuicio a intereses legítimos del afectado o de terceros. Esta previsión no se recoge en el nuevo reglamento pero el autor entiende que se puede aplicar en aplicación de normas generales de nuestro ordenamiento jurídico.

Más allá de la aplicabilidad o no de esta excepción, lo que realmente llama la atención de la citada declaración de inconstitucionalidad es que se haya entendido inconstitucional la previsión citada y que preceptos que hoy día siguen vigentes no fueran tachados en su momento con el mismo defecto. Si bien se ha aceptado en alguna ocasión la mayor determinación de los preceptos que se analizan con respecto a los que han sido declarados inconstitucionales[3150], no se entiende aquí cómo se considera que el concepto de "intereses más dignos de protección" constituye una expresión excesivamente ambigua y, por lo tanto, contraria a Derecho, y, en cambio, el concepto de "derechos y libertades de terceros" no. Ciertamente, no parece que el contenido de ambos conceptos sea esencialmente distinto. En ambos casos la indeterminación es significativa y merecen una valoración negativa.

II. DERECHO DE ACCESO.

II.1. La regulación del derecho de acceso en la normativa de protección de datos.

Antes de analizar las particularidades que presenta el ejercicio del derecho de acceso en el ámbito sanitario es necesario aclarar el contenido de las normas que regulan la protección de datos al respecto de este derecho, pues esta aclaración ayudará a solucionar los problemas de interpretación que surgen de la aplicación de esta normativa en el concreto ámbito sanitario.

II.1.1. La importancia del derecho de acceso.

La LOPD recoge una regulación específica del derecho de acceso, siguiendo lo que ya disponían la Directiva europea[3151] y el Convenio del Consejo de Europa de 1981[3152]. Señala la Ley que el interesado tiene derecho a pedir y obtener información sobre los datos de carácter personal que le conciernen y que están siendo objeto de tratamiento por el responsable ante quien se realiza la solicitud. La Ley se refiere concretamente a la posibilidad de obtener información sobre qué datos se están manipulando, el origen de dichos datos y las comunicaciones que se hayan realizado o se vayan a realizar de los mismos. Este ejercicio será gratuito para el titular de los datos[3153]. La Ley fija también cómo ha de ejercerse este derecho de acceso. Se señala que la información solicitada podrá obtenerse mediante la consulta de la misma a través de su visualización, a través de un escrito, copia, telecopia o fotocopia, certificada

[3150] GUICHOT, *Datos personales…,* cit., 2005, p. 408.

[3151] Artículo 12 Directiva: "*Los estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: -la información de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; -La comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; -El conocimiento de la lógica utilizada en los tratamientos automatizados de los datos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15*".

[3152] Artículo 8.b) Convenio 108/1981 del Consejo de Europa: "*Cualquier persona deberá poder:*
obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible".

[3153] Artículo 15.1 LOPD: "*El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos*".

o no, en forma legible e inteligible. En todo caso la información solicitada deberá poder obtenerse con facilidad, sin tener que emplear claves o códigos que requieran el empleo de mecanismos, sobre todo informáticos, complejos[3154]. Por último, la Ley establece un límite temporal para poder ejercer el derecho de acceso. Sólo podrá ser ejercitado a intervalos no inferiores a un año. Es decir, han de transcurrir como mínimo doce meses entre acceso y acceso ejercido por el mismo interesado. Sólo en caso de que el titular de los datos pueda alegar intereses legítimos que lo justifiquen podrá ejercer el acceso en intervalos inferiores[3155]. La regulación contenida en la LOPD se concreta en el RDLOPD, que desarrolla los citados puntos.

De lo expuesto por las normas se deduce que el derecho de acceso no es otra cosa que la facultad de conocer por parte de una persona lo que está sucediendo con sus datos cuando son manipulados por un responsable. Antes de nada hay que aclarar, que no hay que confundir esta facultad con el derecho reconocido en el ordenamiento administrativo a conocer, en términos genéricos, la información contenida en registros y documentos que obran en los archivos administrativos[3156]. Esta distinción ya se subrayó en su día en el ámbito europeo con motivo de la aprobación de la Directiva relativa a la reutilización de la información del sector público[3157]. El RDLOPD refrenda esta distinción[3158]. Ya se han señalado al analizar la cesión de datos algunas de las características más importantes de esta última facultad. Constituye un derecho general de la ciudadanía para conocer los documentos con los que cuenta la Administración, que a veces recogen datos de carácter personal. La principal finalidad de este derecho consistiría en hacer efectivos los principios de transparencia y publicidad, y controlar así la actividad de las administraciones. El derecho de acceso al que ahora se va a hacer referencia no tiene como fin, no por lo menos como fin principal, el control por parte de una persona sobre la Administración, sino el control de una persona sobre sus propios datos.

El derecho de acceso constituye sin lugar a dudas la facultad más relevante con la que cuenta el titular de los datos de entre las reguladas en el Título III de la Ley[3159]. En este sentido, se ha puesto de manifiesto en alguna resolución de la AEPD que "no contestar al ejercicio del

[3154] Artículo 15.2 LOPD: "*La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos*".

[3155] Artículo 15.3 LOPD: "*El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes*".

[3156] FERNÁNDEZ SALMERÓN y VALERO TORRIJOS, "La Difusión de Información…", cit., 2008, hacen hincapié en esta distinción.

[3157] Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, 7/2003, sobre la reutilización de la información del sector público y la protección de datos personales, 12 de diciembre de 2003: Distingue el derecho de acceso que reconoce la Directiva y el acceso a los documentos del sector público en el marco de la legislación sobre libertad de información y la puesta a disposición de información del sector público que contiene datos personales con fines de reutilización. Esto viene a cuento de la aprobación de la Directiva 2003/98/CE del parlamento Europeo y del Consejo, 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.

[3158] Artículo 27.3 RDLOPD: "*El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común*".

[3159] PUENTE, "Derechos de las personas…", cit., 2008, p. 297; ARENAS RAMIRO, "El derecho de acceso…", cit., 2010, p. 1.161.

derecho de acceso impide que el afectado pueda tener el control sobre sus datos"[3160]. Esta relevancia se deja entrever, también, en el articulado de la LOPD, que exige expresamente que "*los datos de carácter personal* (sean) *almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados*"[3161]. Esta previsión requiriendo facilitar el ejercicio del derecho de acceso deja adivinar su importancia. No hay que olvidar tampoco que el acceso es la facultad más ejercida por los ciudadanos[3162].

Esta especial consideración del derecho de acceso deriva de dos circunstancias. A) En primer lugar, del hecho de que, desde un punto de vista práctico, constituye la prerrogativa esencial para que una persona conozca los datos que un responsable de fichero posee sobre su persona y las circunstancias que rodean a la manipulación que dicho sujeto realiza de esa información[3163]. De esta forma su ejercicio se convierte, tal y como han señalado los tribunales en alguna ocasión, en condición previa para la realización de la mayoría de los otros derechos de la persona, como por ejemplo la cancelación y la rectificación[3164]. Es cierto, como dice el RDLOPD, que los diferentes derechos a los que ahora se hace referencia son independientes, con entidad y relevancia propia. Sin embargo, la consideración que hace la norma de que "*no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro*"[3165], no es del todo acertada. En la práctica no pueden ejercerse los derechos de rectificación o cancelación sin que el titular de los datos tenga conocimiento de los datos que el responsable posee[3166]. Si bien dicho conocimiento podría llegar mediante el ejercicio del derecho de información[3167], en la mayoría de casos será necesario el acceso a los datos para poder ejercer después la cancelación o la rectificación. No hay que perder de vista que el derecho de acceso permite un acercamiento directo a los datos que se están manipulando, mientras que el derecho a la información no lo hace, limitándose al conocimiento de los parámetros que rodean al tratamiento de los datos. Es por ello que cuando en algún caso se ha pretendido ejercer el

[3160] Resolución R/00818/2005, de 18 de enero de 2006, procedimiento PS/00131/2005. PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 278: "se configura como uno de los ejes fundamentales sobre los que se articula la protección del honor, la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, en desarrollo de lo dispuesto en el artículo 18.4 de la Constitución Española".

[3161] Artículo 4.6 LOPD. Artículo 8.7 RDLOPD: "*Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación*".

[3162] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 278.

[3163] STSJ de Madrid 17 de mayo de 2000, FJ 3: "el derecho de acceso (...) es el derecho a solicitar y obtener información de los datos de carácter personal incluidos en los ficheros automatizados".

[3164] STC 20 de julio de 1993, FJ 4: "los riesgos derivados del exceso, de los errores, o del uso incontrolado de información de carácter personal no pueden ser afrontados eficazmente por los particulares afectados a causa de una información insuficiente, pues los ciudadanos se encuentran inermes por la imposibilidad de averiguar qué información sobre sus personas almacenan las distintas Administraciones Públicas, premisa indispensable para cualquier reclamación o rectificación posterior". PALOMAR OLMEDA, "Los Derechos Personales…", cit., 2007, p. 28.

[3165] Artículo 24.1 RDLOPD.

[3166] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 254: da a entender que en la práctica sólo después de ejercer el derecho de acceso se podrá ejercer el bloqueo, la cancelación o rectificación; EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 157; SERRANO PÉREZ, "Los derechos de rectificación…", cit., 2010, pp. 1.229-1.230

[3167] PUENTE, "Derechos de las personas…", cit., 2008, pp. 263-264.

acceso y la cancelación simultáneamente, se ha concretado que primero deberá ejecutarse el derecho de acceso y después la cancelación[3168].

B) En segundo lugar, la relevancia deriva del hecho de que, como ya se dijera más arriba, el derecho de acceso, en relación con los derechos de información y de consulta al Registro General de Protección de Datos, constituye la base para que el titular de los datos pueda conocer en todo momento los parámetros entre los que se están manipulando los datos que le conciernen[3169]. Estos tres derechos configuran un triángulo de facultades que posibilitan que el interesado conozca las circunstancias que rodean a todo tratamiento: antes de que se inicie la manipulación con el derecho a la información, y después con el derecho de acceso y derecho de consulta. El derecho de acceso es además el que mayor control otorga al titular de los datos, pues supone acceder directamente a la información que el responsable tiene sobre el titular, mientras que en los otros casos simplemente se darán a conocer las principales características que rodean la manipulación de los datos. El derecho de acceso posibilita que se tenga conocimiento exacto de los datos que se están manipulando y de las circunstancias que rodean a estas operaciones en cualquier momento, lo cual es imprescindible para hacer efectivo el control que deriva del derecho a la autodeterminación informativa.

II.1.2 El ejercicio del derecho de acceso.

El ejercicio de este derecho no presenta grandes particularidades con respecto a las características comunes que se han expuesto más arriba sobre el ejercicio de los derechos de las personas. Sin embargo, hay ciertos puntos que merecen ser comentados y que han sido desarrollados en gran parte por el RDLOPD. A) El ejercicio del derecho, como reconoce la LOPD, es gratuito. Es de agradecer que la nueva Ley haya dispuesto este carácter gratuito expresamente en contraposición a lo que hacía la LORTAD, que no disponía nada al respecto[3170].

B) La realización del derecho, según reconoce la Ley, puede llevarse a cabo de distintas formas. Se abrazan diversas alternativas para que pueda hacerse efectivo de la manera más sencilla posible. Esta regulación es coherente con la previsión que hace la normativa de facilitar el ejercicio del derecho de acceso. El reglamento que desarrolla la Ley concreta las vías por las que se puede hacer efectivo: visualización en pantalla; escrito, copia o fotocopia remitida por correo, certificado o no; telecopia; correo electrónico u otros sistema de comunicación electrónicas; y añade una cláusula genérica: cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable. El titular de los datos podrá elegir entre estas vías[3171]. Los tribunales han subrayado esta facultad del titular de elegir el medio que desee para recabar la información a la que quiere

[3168] Resolución AEPD R/01219/2009, 12 de mayo de 2009, procedimiento TD/01674/2008.
[3169] GONZÁLEZ MURUA, "Comentario a la STC...", cit., 1993, pp. 239-245, analiza la relación entre el derecho de acceso y el derecho a la información al hilo de lo establecido en la STC 254/1993; GAY FUENTES, *Intimidad y Tratamiento...*, cit., 1995, p. 86, incluso incluye dentro del derecho a la información al derecho de acceso.
[3170] COLLADO GARCÍA-LAJARA, *Protección de Datos...*, cit., 2000, pp. 40-41.
[3171] Artículo 28.1 RDLOPD. PUENTE, "Derechos de las personas…", cit., 2008, p. 309.

acceder[3172]. Esta facultad de elegir viene limitada, sin embargo, por una serie de condicionantes recogidos en el reglamento. Las vías de consulta podrán restringirse en función del formato del fichero que contiene los datos o la naturaleza del tratamiento, siempre y cuando se garantice al titular de los datos una vía de acceso gratuita y que asegure la comunicación escrita si éste así lo exige[3173]. En la misma línea, si el titular de los datos exige que el responsable facilite el acceso a través de un medio concreto, semejante al ofrecido por el responsable pero que conlleva un coste desproporcionado, será el titular de los datos quien se hará cargo de dichos costes[3174]. De esta regulación se desprende la idea de que el ejercicio del derecho de acceso se llevará a cabo teniendo en cuenta, sobre todo, los medios técnicos con los que cuenta el responsable del fichero. Evidentemente, el responsable estará obligado, salvo limitación justificada, a hacer efectivo el derecho de acceso en toda su extensión. Sin embargo, en la medida en que se respete esta premisa, podrá ofrecer diferentes alternativas al titular de los datos, pero si este último quiere ejercer el acceso a través de una fórmula diferente que supone un coste desproporcionado, el responsable no estará obligado a asumir dicho coste. En todo caso, este último deberá garantizar que en el ejercicio del acceso se respetan las medidas de seguridad debidas, para que la información no sea sustraída, alterada o perdida. Si el titular de los datos rechaza la vía de acceso que le ofrece el responsable, este último no responderá de los riesgos que para la seguridad de la información pudieran surgir[3175]. Es lógico que si el titular de los datos elige ejercer el acceso a través de una vía diferente a la propuesta por el responsable, el primero asuma los riesgos que puedan derivar del empleo de ese sistema.

C) En cuanto al contenido de la información, señala el reglamento que el derecho de acceso abarca la facultad del titular de conocer si sus datos están siendo tratados, cuál es la finalidad de dicha manipulación, cuál es el origen de los datos y si se han realizado o se van a realizar comunicaciones de los mismos[3176]. Además, especifica que la información no se referirá solamente a los datos de base, sino que abrazará también a la información que haya podido resultar del tratamiento de dichos datos de base[3177]. El titular podrá solicitar información sobre unos datos concretos que le conciernen o sobre la totalidad de los datos con los que el responsable del fichero cuenta sobre dicho titular[3178]. El responsable deberá dar la información de forma legible e inteligible, de fácil acceso, sin que se dificulte el ejercicio del derecho[3179].

Se observa que se trata de otorgar al titular de los datos una radiografía completa de las operaciones que se han llevado a cabo con sus datos, de tal forma que el control sobre los mismos sea, en principio, absoluto[3180]. En algún caso se ha subrayado que la intencionalidad de la normativa es dar un sentido amplio al derecho de acceso. Y no sólo se trata de que se otorgue la mayor información posible, es decir, información sobre el máximo de los aspectos posibles en

[3172] SAN 27 de octubre de 2006, FJ 7.
[3173] Artículo 28.2 RDLOPD.
[3174] Artículo 28.3 RDLOPD.
[3175] Artículo 28.3 RDLOPD.
[3176] Artículo 27.1 RDLOPD.
[3177] Artículo 29.3 RDLOPD.
[3178] Artículo 27.2 RDLOPD.
[3179] Artículo 29.3 RDLOPD.
[3180] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 279: concibe el derecho de acceso con un objeto muy amplio, que abarca toda la información posible sobre el tratamiento.

relación al tratamiento, sino también con el mayor de los detalles, sin que la información pueda ser en ningún momento vaga e indeterminada[3181]. Sin embargo, se han puesto ciertas limitaciones al ejercicio de este derecho de acceso considerado de inicio de forma tan amplia.

Primero, si bien parece darse un sentido especialmente amplio al alcance del derecho de acceso, en algún caso se ha venido a limitar en la práctica dicha amplitud. Se ha dispuesto, por ejemplo, que el derecho de acceso no abarca la facultad de conocer la identidad de todas las personas que han accedido a los datos concernientes al titular. Una cosa es que tenga derecho a conocer las cesiones que se han llevado a cabo y otra que tenga acceso a la identidad de todas las personas que han conocido dichos datos[3182]. En este caso, tanto tribunales como la AEPD consideran que el alcance del derecho de acceso debe verse limitado en la práctica. Se entiende acertada esta interpretación, pues lo contrario podría llevar a situaciones extremadamente complejas para los responsables de los ficheros, que podrían verse sometidos a una tarea desorbitada de investigación para satisfacer la curiosidad de un titular de datos de conocer todos los detalles sobre el uso que se da a sus datos. Se interpreta que el derecho de acceso tiene un amplio alcance, pero que se agota con el contenido fijado en la Ley y el reglamento que la desarrolla. Este límite, sin embargo, deberá entenderse en sentido estricto y no podrá llevar a restringir el derecho de los titulares de los datos a conocer los destinatarios de las cesiones, es decir, los órganos responsables del tratamiento[3183]. Por ejemplo, una cosa es que en un centro sanitario el titular de unos datos conozca el órgano responsable de un fichero y otra que tenga derecho al acceso de la identidad de todos los profesionales que han empleado dicha información. Esta segunda posibilidad multiplicaría la labor de los responsables de los ficheros hasta límites desproporcionados. Segundo, como se dijera más arriba, cuando la operación plantee cierta complejidad para el responsable el afectado o interesado deberá facilitar la labor de aquél concretando el fichero sobre el que se quiere ejercer el derecho[3184]. No se especifica en el reglamento cuándo se entiende que existen las razones de especial complejidad a las que se alude. Simplemente se señala que la complejidad ha de ser especial, no bastando que sea un sistema mínimamente complicado. Normalmente la complejidad derivará, se entiende aquí, del hecho de que exista un número muy alto de ficheros que haga difícil la localización de los datos a los que el titular solicita acceder. En algún caso la doctrina ha citado el caso de la videovigilancia, donde pueden encontrarse multitud de grabaciones[3185].

[3181] Resolución AEPD R/00459/2005 27 de julio de 2005, procedimiento PS/00068/2005: en relación al derecho de acceso: este derecho no se completa con una vaga información, sino que ha de concretarse en una información determinada sobre qué datos se están manipulando, de dónde vienen esos datos, etc. Sobre todo, se hace hincapié en el origen de los datos, que es lo que la mayoría quiere saber, ¿de dónde vienen los datos que una empresa está manipulando? La información sobre el origen ha de ser concreta, no vale con remitirse, como se hizo en este caso particular, a los "listados accesibles al público –páginas blancas, páginas amarillas, QDQ, repertorios de servicios de telecomunicaciones…"

[3182] SAN 30 de noviembre de 2005, FJ 4: de acuerdo a lo que ya había señalado antes la AEPD, concluye el tribunal que el derecho de acceso reconoce la facultad de conocer las posibles cesiones que se hayan podido dar a otros responsables de fichero, pero del artículo 15 no se reconoce el derecho a conocer los accesos que dentro de la organización del responsable se hayan podido dar. Informe jurídico AEPD 0167/2005, en el mismo sentido.

[3183] STS 7 de julio de 2009, FJ 2.

[3184] Artículo 27.2 RDLOPD. ARENAS RAMIRO, "El derecho de acceso…", cit., 2010, p. 1.165.

[3185] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, pp. 289-290: la posibilidad que se prevé en el 27 RDLOPD de que el responsable pueda exigir al titular que concrete sobre qué datos quiere ejercer el acceso cuando

D) El ordenamiento establece un límite de relevancia al ejercicio del derecho de acceso. Como apuntaba la Ley, también el reglamento dispone que sólo se puede ejercer este derecho en intervalos superiores a un año, salvo cuando el titular demuestre la existencia de un interés legítimo para ejercer el acceso en un espacio temporal más breve[3186]. Evidentemente, fuera de esos casos en que existe dicho interés justificado, queda en manos del responsable denegar o permitir el acceso cuando no ha transcurrido el plazo de un año[3187]. El responsable, dentro de esos doce meses entre acceso y acceso, puede denegar dicho ejercicio, pero puede no hacerlo.

En principio, parece tener sentido que el ejercicio del derecho esté sujeto a determinadas condiciones, pues lo contrario podría acarrear un abuso en su ejercicio, imposible de satisfacer por parte del responsable del fichero[3188]. Sin embargo, la regulación de la normativa estatal ha sido criticada. La fijación de un plazo de doce meses para controlar el ejercicio del derecho es rechazable[3189], más hoy en día cuando las nuevas tecnologías hacen más fácil establecer mecanismos por los que puede satisfacerse el derecho de acceso de los titulares de los datos[3190]. En el ámbito sanitario, por ejemplo, la historia clínica electrónica debería facilitar el ejercicio de este derecho[3191]. Es especialmente criticable la redacción de la Ley en el punto en que establece como excepción al cumplimiento de ese plazo la presentación de un "interés legítimo" por parte del titular de los datos. ¿Qué se entiende por interés legítimo? ¿No constituye suficiente argumento para ejercer el derecho de acceso el hecho de que el titular quiera conocer lo que sucede con sus datos? ¿Cómo acreditar ese interés? Todas estas interrogantes quedan en el aire en la normativa. Por otro lado, se sobreentiende de la redacción de las normas que sería el responsable del fichero el que determinaría si existe o no el interés legítimo[3192], lo cual le otorgaría un margen de apreciación que no le corresponde[3193], pues le atribuiría la facultad de limitar el ejercicio del derecho de acceso, atendiendo a criterios propios sobre la existencia o no de intereses legítimos.

La Directiva europea reguladora de la protección de datos de carácter personal señala la posibilidad de ejercer el derecho de acceso con una "periodicidad razonable". En este sentido, la LOPD sigue la directriz marcada por la UE. Sin embargo, la redacción de la Ley se erige en verdaderamente rigurosa. Se entiende aquí que quizás hubiera sido más afortunado seguir la redacción más flexible aportada por la norma europea. Hay que tener en cuenta que en

existe cierta complejidad se ve como acertada. Pone como ejemplo el caso de la videovigilancia, donde puede haber multitud de grabaciones sobre una persona.

[3186] Artículo 30.1 RDLOPD.

[3187] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 284.

[3188] GUICHOT, *Datos Personales...,* cit., 2005, p. 398, nota al pié nº 670: "El sentido de la prescripción es claro, y consiste en proscribir las consultas demasiado frecuentes que pueden entorpecer y encarecer la actividad del responsable del tratamiento". SAN 9 de noviembre de 2005, FJ 3, justifica la denegación del ejercicio del derecho de acceso por pretender realizarlo en un plazo inferior a doce meses.

[3189] DAVARA RODRÍGUEZ, *Manual de Derecho...*, cit., 2005, p. 94.

[3190] TRONCOSO REIGADA, *Protección de Datos...,* cit., 2008, p. 68: viene a apuntar que el intervalo de doce meses para ejercer el derecho de acceso tiene sentido cuando es complicado que el responsable pueda llevarlo a cabo, pero en la actualidad las TIC facilitan la realización de dicho derecho.

[3191] Documento de Trabajo del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE, sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007.

[3192] SERRANO PÉREZ, *El Derecho...*, cit., 2003, p. 353.

[3193] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 284.

situaciones diferentes el acceso continuo a los datos puede resultar más o menos justificado. Por ejemplo, en casos en que existe una relación constante entre responsable y titular de los datos el titular puede querer llevar a cabo un control más cercano de lo que ocurre con sus datos. Que este interés por controlar los datos por parte del titular se vea limitado por la fijación de determinados plazos no parece tener sentido. La limitación debería basarse en argumentos más sólidos, que atendieran a las circunstancias de cada caso, que la mera fijación por Ley de un plazo. En todo caso, la norma debería concretar con mayor precisión lo que se debe entender por "interés legítimo"[3194]. La doctrina ha entendido por interés legítimo, por ejemplo, el tener indicios de que el tratamiento de datos que está llevando a cabo el responsable es contrario a Derecho[3195]. También desde la doctrina, como posible solución práctica que abra la posibilidad de ejercer el acceso en intervalos inferiores de tiempo, se ha apuntado el cobrar los accesos que se realicen antes del transcurso de los doce meses impuestos por el ordenamiento[3196]. Puede ser una solución, acorde con lo que dispone la Directiva sobre la posibilidad de cobrar el ejercicio del derecho[3197], aunque estaría en desacuerdo con lo que dispone la LOPD con respecto a la gratuidad del mismo.

Sea como fuera, y más allá de la adecuación de la fijación de un plazo determinado, se entiende aquí que lo más acorde con el principio *favor libertatis* y con la obligación de afectar en la menor medida posible el derecho a la autodeterminación informativa, hubiera sido que la normativa fijara una regulación en la que fuera el responsable quien tuviera que justificar la razón por la que limita el derecho, a saber: esfuerzo desproporcionado, coste elevado, etc., y no que haya de ser el propio titular de los datos quien deba justificar el ejercicio de su derecho. No parece acorde a los principios citados que la regla general la constituya la limitación al ejercicio de la autodeterminación informativa y que la posibilidad de hacer efectivo este derecho sea la excepción.

E) La normativa fija el proceso a seguir por el titular de los datos para el ejercicio del derecho de acceso. La solicitud deberá hacerse como establece el reglamento en la regulación común al ejercicio de los derechos de acceso, cancelación, rectificación y oposición. Sin embargo, parece que los tribunales han aceptado cierta flexibilidad, de manera que aunque no se respete la fórmula recogida exactamente por la normativa se deberá aceptar la solicitud si las pretensiones del titular quedan claras[3198]. Una vez realizada la solicitud el responsable del fichero tendrá un mes a contar desde la recepción de la solicitud para resolverla. En caso de que el responsable no cuente con información sobre quien realiza la solicitud tendrá la obligación de comunicárselo en dicho plazo. Parece clara la voluntad del legislador de garantizar en todo caso el control de los ciudadanos sobre sus datos. Si transcurre el mes sin recibir respuesta la normativa prevé la

[3194] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 349: el que el acceso se haya de llevar a cabo a intervalos superiores a doce meses responde a la necesidad de que el responsable no se vea acosado. Puede aminorarse el intervalo cuando haya interés legítimo. El concepto interés legítimo ha sido interpretado de manera amplia por el TS y TC.
[3195] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 252.
[3196] DAVARA RODRÍGUEZ, *Manual de Derecho...*, cit., 2005, p. 95.
[3197] Artículo 12 Directiva 95/46/CE, habla de la posibilidad de reconocer un derecho de acceso no sujeto a "gastos excesivos".
[3198] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 374.

posibilidad a favor del solicitante para que interponga reclamación de tutela de los derechos[3199]. Así, el silencio juega en contra del titular de los datos. Si cuando no se ha recibido respuesta la única alternativa es interponer una reclamación será porque se entiende que se ha rechazado la solicitud. De lo contrario, la reclamación no tendría sentido. Esta interpretación es acorde a lo que fijaba el reglamento de desarrollo de la derogada LORTAD, que reconocía expresamente el silencio negativo en estos casos[3200].

El hecho de que se asuma que el silencio en este punto será negativo se entiende contrario, en lo que toca a la Administración, a lo que dispone a este respecto la LPAC[3201], que fija la regla general de reconocer el carácter positivo del silencio para estos casos. Un reglamento en ningún momento puede contradecir lo dispuesto en la citada Ley. Por lo tanto, y a pesar de lo que pueda decir la disposición general, en principio se debería entender que el silencio en este supuesto es positivo. En cualquier caso, como ha puesto de manifiesto la doctrina, a efectos prácticos el silencio negativo o positivo tendría el mismo resultado, pues en el segundo caso también el titular de los datos se quedaría sin acceder a los datos[3202]. Es por ello que la inactividad del responsable del fichero ante una solicitud puede ser sancionada. La Ley reclama en todo caso la actuación o la respuesta del responsable[3203]. Los tribunales han entendido que con el silencio no se satisface el derecho de acceso[3204]. Concretamente, han señalado que es difícil imaginar mayor incumplimiento de este derecho, al igual que de los derechos de rectificación o cancelación, que la desatención al ejercicio de dichos derechos[3205]. Esta desatención podría constituir un hecho sancionable[3206].

Si la resolución es estimatoria, el responsable puede remitir en el mismo momento en que estima la solicitud la información solicitada por el titular de los datos o, remitir primero la comunicación de que se ha estimado la solicitud del interesado y luego, en plazo de los diez días siguientes a la comunicación, hacer efectiva la información. El cómputo de este plazo se

[3199] Artículo 18.2 LOPD: "*El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación*".

[3200] Artículo 12.3 RD 1332/1994: *"El responsable del fichero resolverá sobre la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud. Transcurrido este plazo sin que de forma expresa se responda a la petición de acceso, ésta podrá entenderse desestimada a los efectos de la interposición de la reclamación prevista en el artículo 17.1 de la Ley Orgánica 5/1992"*.

[3201] Artículo 43.2 LPAC: "*Los interesados podrán entender estimadas por silencio administrativo sus solicitudes en todos los casos, salvo que una norma con rango de Ley o norma de Derecho Comunitario Europeo establezca lo contrario (...)"*.GUICHOT, *Datos personales…,* cit., 2005, p. 405.

[3202] GUICHOT, *Datos personales…,* cit., 2005, p. 405: sin embargo, en la práctica no tiene fácil solución, pues el silencio positivo dejaría al titular de los datos igual: sin acceso, cancelación…, y debería acudir a la justicia ordinaria por inactividad (25 LJCA).

[3203] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 285, el ordenamiento exige del responsable que se pronuncie mediante escrito, copia, teletipo… de forma legible e inteligible.

[3204] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 354.

[3205] SAN 14 de diciembre de 2006, FJ 3: "no parece posible mayor impedimento que la absoluta desatención al ejercicio del derecho de acceso de modo tal que se convierte dicho derecho en inútil o completamente ineficaz".

[3206] Artículo 44.3 LOPD: "*Son infracciones graves: e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada*". SAN 14 de diciembre de 2006, FJ 4: una cosa es que el responsable ejecute el acceso de manera incompleta o con algún defecto, caso en que la Tutela ante la Agencia puede llevar a corregir dicho ejercicio. Y otro es que ni siquiera se dé una contestación por parte del responsable, caso en que la actividad puede ser perfectamente sancionable.

realizaba, hasta la entrada en vigor del RDLOPD, teniendo en cuenta si el responsable del fichero tenía carácter público o privado. En el primer caso había que atender a lo que establece la LPAC, que señala que en los plazos establecidos en días deberán tenerse en cuenta, salvo que se diga lo contrario, los días hábiles[3207]. En el segundo caso había que atender a lo que fija el Código Civil, lo que llevaba a que en el caso en que el responsable del fichero fuera privado el plazo se computara en días naturales[3208]. Este criterio se ha seguido expresamente también por alguna resolución de la AEPD[3209]. Hoy, el reglamento que desarrolla la Ley dispone que en los plazos fijados por días sólo se computarán los días hábiles, mientras que los plazos marcados por meses se computarán de fecha a fecha[3210].

F) Por último, las excepciones al ejercicio del derecho de acceso son las comunes dispuestas en la LOPD para todos los derechos. Sin embargo, el reglamento que desarrolla la Ley reconoce la posibilidad de que otras leyes o normas comunitarias dispongan nuevas excepciones que justifiquen que el responsable del fichero deniegue el acceso[3211]. En todo caso, cuando se deniegue la solicitud, el responsable estará obligado a hacer saber al titular de los datos su derecho a acudir ante la agencia de protección de datos correspondiente para recabar, en su caso, la tutela de dicha institución[3212].

II.2. El derecho de acceso en el ámbito sanitario.

Analizados brevemente los puntos más importantes de la regulación del derecho de acceso en la normativa de protección de datos, se observarán en los siguientes apartados cuáles son los problemas que presenta la aplicación de esta normativa en el ámbito sanitario y qué límites se imponen desde la normativa sanitaria a este derecho.

II.2.1. El reconocimiento en la normativa sanitaria de distintos instrumentos dirigidos a garantizar que el titular de los datos acceda a la información que le concierne.

En el ámbito específicamente sanitario, el derecho de acceso adquiere una relevancia especial, tal como puede deducirse simplemente atendiendo a la abundante doctrina que se ha dedicado a analizar el derecho de acceso del paciente a su historia clínica. Esta relevancia se deduce desde una doble perspectiva. Por un lado, desde el punto de vista del derecho a la

[3207] Artículo 48.1 LPAC: "*Siempre que por Ley o normativa comunitaria europea no se exprese otra cosa, cuando los plazos se señalen por días, se entiende que éstos, son hábiles, excluyéndose del cómputo los domingos y los declarados festivos"*.

[3208] Artículo 5.2 CC: "*En el cómputo civil de los plazos no se excluyen los días inhábiles*".

[3209] Resolución de la AEPD R/00731/2004, de 30 de diciembre de 2004, procedimiento TD/00276/2004. Informe jurídico AEPD 534/2003: los criterios para computar los plazos de cancelación y rectificación de la LOPD se computan en base a 48 LPAC, cuando el tratamiento se realiza por administraciones. En los demás se aplicará el CC, artículo 5. En estos plazos deben hacerse efectivos la cancelación y la rectificación: hacer efectivo significa llevar a cabo la rectificación y cancelación y notificar este hecho a los interesados.

[3210] Artículo 6 RDLOPD. ARENAS RAMIRO, "El derecho de acceso…", cit., 2010, p. 1.182.

[3211] Artículo 30.2 RDLOPD: "*Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso*".

[3212] Artículo 30.3 RDLOPD: "*En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre*".

autodeterminación informativa, el acceso se erige en pieza fundamental para que el titular de los datos pueda controlar lo que sucede con los datos de carácter personal que le conciernen, que en este caso afectan, en muchas ocasiones, a la esfera más íntima de las personas. Por otro, desde el punto de vista del derecho a la protección de la salud, el acceso constituye un elemento indispensable para que el paciente conozca cuál es su estado de salud y pueda tomar las decisiones oportunas en relación a ésta[3213]. En la actualidad, el principio de autonomía que rige la relación médico-paciente exige que el paciente tenga conocimiento sobre su estado de salud[3214]. Si se reconoce que hoy día el usuario del sistema sanitario se erige en sujeto activo a la hora de tomar las decisiones que le conciernen, será necesario que tenga acceso a la información que le concierne y a los tratamientos que de la misma se realicen en un sistema sanitario determinado para poder ejercer dicha autonomía.

Si bien desde el punto de vista del derecho a la autodeterminación informativa lo que principalmente interesa es analizar el derecho de acceso como medio de conocer y controlar la información que concierne a cada uno, desde la perspectiva de la defensa del derecho a la salud, el acceso a la historia clínica tiene relevancia con fines sanitarios[3215]. En todo caso, y si bien se puede hablar de dos perspectivas diferentes, lo cierto es que en última instancia ambas están interrelacionadas. Ejemplo de ello es que la protección de la salud puede condicionar el ejercicio del derecho de acceso, entendido como facultad que completa el derecho a la autodeterminación informativa.

En el ámbito sanitario el derecho de acceso se traduce la mayoría de ocasiones como la facultad de acceder a la historia clínica. Si bien es cierto que gran parte de la información sobre los pacientes se recoge en la historia clínica, y que dicho documento es el más relevante, no es menos cierto que no sólo en la historia clínica se recoge información sanitaria en este sector. Ficheros administrativos que contienen datos de carácter personal, informes que se guardan en los ficheros de especialistas, entre otros, son comunes en los centros sanitarios. No hay más que ver las normas que crean los ficheros de los diferentes sistemas sanitarios, caso de Osakidetza, que se ha citado en numerosas ocasiones durante este trabajo. Aunque la normativa exige que la información sanitaria de cada paciente se recoja de acuerdo con el principio de integración en el sistema sanitario[3216], lo cierto es que son diferentes los ficheros que se crean en estos sistemas.

[3213] MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, p. 37: el derecho de acceso a la información sanitaria de una persona no sólo deriva del derecho a la protección de datos, sino también del derecho a la protección de la salud.

[3214] Texto de Acuerdo del Consejo Interterritorial sobre Consentimiento Informado, adoptado en la sesión plenaria del 6 de noviembre de 1995, reconoce que "la información recibida por el paciente debe entenderse como un proceso gradual y continuado a lo largo de todo el proceso asistencial, que se realiza en el seno de la relación médico-enfermo durante todo el proceso, y que debe permitir que el paciente participe activamente en el proceso de toma de decisiones respecto al diagnóstico y tratamiento de su enfermedad".

[3215] ANTEQUERA VINAGRE, "Historia Clínica...", cit., pp. 18-19, "son muchos los motivos por los cuales un paciente o un familiar acude a una Unidad de Atención al Paciente a pedir copia de su HC:
a) el hecho de conocer una segunda opinión facultativa,
b) el hecho de ir a otro servicio sanitario para que le vea un especialista.
c) porque es un paciente transeúnte y desea la copia para llevarla a su médico.
d) para conocer si existe posibilidad de reclamación judicial".

[3216] Artículo 15.4 LBAP: "*La historia clínica se llevará con criterios de unidad y de integración, en cada institución asistencial como mínimo, para facilitar el mejor y más oportuno conocimiento por los facultativos de los datos de un determinado paciente en cada proceso asistencial"*.

En todo caso, cuando se hable aquí del derecho de acceso en el ámbito sanitario o del derecho de acceso a la historia clínica, se entenderá que los criterios aportados son válidos para el acceso a cualquiera de los ficheros.

La regulación del derecho de acceso en este ámbito se produce a través de la normativa de protección de datos y de la normativa sanitaria. En relación a las normas dedicadas a regular la protección de datos de carácter personal las referencias al ejercicio del derecho de acceso en el campo sanitario son prácticamente inexistentes en el ámbito estatal. No ocurre lo mismo en el ámbito internacional. La Directiva, si bien en su articulado no hace ninguna referencia a esta cuestión, en sus considerandos entra a precisar algunos puntos sobre el acceso a los datos sanitarios. Señala en concreto que "*(…) en interés del interesado de que se trate y para proteger los derechos y libertades de terceros, los Estados miembros podrán limitar los derechos de acceso y de información; que podrán, por ejemplo, precisar que el acceso a los datos de carácter médico únicamente pueda obtenerse a través de un profesional de la medicina*"[3217]. Por su parte, la Recomendación del Consejo de Europa sobre la protección de datos médicos recoge una completa regulación de este derecho. Reconoce, entre otros, la facultad del titular de acceder a sus datos médicos. Señala, sin embargo, que el acceso se deberá llevar a cabo a través de un profesional sanitario o, si está permitido por el ordenamiento interno, a través de una persona designada por el titular de los datos. La información deberá darse al titular de los datos de manera inteligible[3218]. Luego, reconoce la norma internacional una serie de limitaciones a este derecho de acceso, que en su mayor parte se prevén en el ámbito interno en la LOPD y en la LBAP. Señala la recomendación que el acceso a los datos médicos se puede limitar si así lo prevé una Ley, si se erige en una medida para proteger la seguridad del Estado, la seguridad pública o para perseguir crímenes, o constituye una medida para proteger la salud del afectado, o para salvaguardar la intimidad de terceros, por ejemplo porque se trata de datos genéticos que puede desvelar información sobre un pariente consanguíneo o uterino o pariente que tiene vínculo directo en línea germinal, o los datos a los que se quiere acceder son utilizados con fines de investigación científica o estadística y se aprecia que dicho tratamiento no va a producir ninguna violación en la intimidad del titular de los datos[3219]. En todo caso, los criterios ya citados, y aportados por la normativa de protección de datos de manera general para todos los accesos, son aplicables en el ámbito sanitario.

La normativa sobre protección de datos ha de ser analizada a la luz de lo que dicta la normativa sanitaria. La regulación en el ámbito sanitario del derecho de acceso se lleva a cabo

[3217] Considerando 42 Directiva 95/46/CE.

[3218] Artículo 8.1 R (97) 5: "*Se permitirá a toda persona el acceso a sus datos médicos, ya directamente o a través de un profesional sanitario o, si lo permite la ley nacional, a través de una persona designada por el titular de los datos. La información debe ser facilitada de modo inteligible*".

[3219] Artículo 8 R (97) 5: "*2. El acceso a los datos médicos puede ser denegado, limitado o rechazado sólo si lo prevé la ley y si: a)Constituye una medida necesaria en una sociedad democrática por su interés en proteger la seguridad del Estado, la seguridad pública o la represión de crímenes; b)El conocimiento de la información es probable que cause un serio daño a la salud del afectado; c)La información sobre el afectado revela también información sobre terceros o, respecto a los datos genéticos, si esta información es probable que cause un serio daño a un pariente consanguíneo o uterino o a una persona que tiene un vínculo directo en línea germinal; o d)Los datos son empleados para fines de investigación científica o estadística y se aprecia con nitidez que no hay riesgo alguno de violación de la intimidad del afectado, especialmente el de usar los datos en decisiones o medidas que afecten a un individuo en particular*".

fundamentalmente en la LBAP y en las normas autonómicas equiparables[3220]. Esta Ley recoge expresamente el derecho del paciente a acceder a la documentación de la historia clínica y a obtener incluso copia de los datos que obran en ella[3221]. Dispone que este derecho puede llevarse a cabo también por representación[3222]. Además, reconoce la norma una serie de limitaciones al ejercicio de dicho derecho. Por un lado, el acceso no podrá ejercerse sobre información que pudiera contenerse en la historia clínica, que afecte a la confidencialidad de los datos de terceras personas distintas al titular de la historia. Por otro, el acceso no podrá afectar a los derechos que los profesionales de la sanidad, que han elaborado la historia clínica puedan tener sobre la información. Estos profesionales pueden oponerse a que los titulares de los datos accedan a las anotaciones subjetivas que hayan podido incluir en la historia clínica[3223]. Esta misma Ley, en otro apartado reconoce el derecho de cada paciente a la información asistencial. Si bien no se califica como derecho de acceso y se regula en un precepto diferente, resulta evidente que esta facultad se vincula con el ejercicio del derecho de acceso. Dispone la LBAP que los pacientes tienen derecho a conocer toda la información sobre su estado de salud y las características que guardan los tratamientos sanitarios que se le van a prestar. Esta información se dará de forma comprensible para el paciente, adecuándose a sus características. Como regla general la información se emitirá por el médico responsable del paciente de forma verbal[3224]. De la misma forma, se reconoce el derecho de los pacientes a no conocer o a no ser informados sobre su salud[3225]. La información la remitirán los propios profesionales sanitarios[3226]. Este

[3220] Artículo 13.1 Ley 21/2000, 29 de diciembre, Catalana, sobre los Derechos de Información concernientes a la Salud y la Autonomía del Paciente, y la Documentación Clínica: "*1. Con las reservas señaladas en el apartado 2 de este artículo, el paciente tiene derecho a acceder a la documentación de la historia clínica descrita por el artículo 10, y a obtener una copia de los datos que figuran en ella. Corresponde a los centros sanitarios regular el procedimiento para garantizar el acceso a la historia clínica. 2. El derecho de acceso del paciente a la documentación de la historia clínica nunca puede ser en perjuicio del derecho de terceros a la confidencialidad de los datos de los mismos que figuran en la mencionada documentación, ni del derecho de los profesionales que han intervenido en su elaboración, que pueden invocar la reserva de sus observaciones, apreciaciones o anotaciones subjetivas. 3. El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación, siempre que esté debidamente acreditada*". Artículo 19 Ley 3/2005, 7 de marzo, de Galicia, de modificación de la Ley 3/2001, 28 de mayo, reguladora del Consentimiento Informado y de la Historia Clínica de los Pacientes: "*1. El paciente tiene el derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuran en la misma. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.*
Este derecho de acceso podrá ejercitarse por representación debidamente acreditada.
4. El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas".

[3221] Artículo 18.1 LBAP: "*El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Los centro sanitarios regularán el procedimiento que garantice la observancia de estos derechos*".

[3222] Artículo 18.2 LBAP: "*El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada*".

[3223] Artículo 18.3 LBAP: "*El derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas"*.

[3224] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, pp. 210 y 219, subraya la necesidad de que sea el médico que asiste al paciente quien remita la información, y señala que la regla general será que la información se remita de forma verbal, si bien se debe dejar constancia de que la información se ha dado con el fin de asegurarse de que el ejercicio de información se ha llevado a cabo efectivamente.

[3225] Artículo 4 LBAP: "*1. Los pacientes tienen derecho a conocer, con motivo de cualquier actuación en el ámbito de su salud, toda la información disponible sobre la misma, salvando los supuestos exceptuados por la Ley. Además, toda*

derecho a ser informado puede verse limitado. El principal límite se prevé para los casos en que el acceso por el paciente a la información sobre su propia salud puede afectar negativamente a la misma. Es decir cabe limitar este derecho por motivos terapéuticos[3227]. La misma regulación se realiza, prácticamente, en el ámbito autonómico[3228].

El derecho de acceso y el derecho a la información, a pesar de regularse en preceptos diferentes de la LBAP, se encuentran estrechamente vinculados en el ámbito sanitario. En alguna ocasión se han confundido, incluso, por los tribunales[3229]. Desde un punto de vista material ambas figuras se dirigen a reforzar la posición del paciente, pues tratan de garantizar que éste controle en todo momento la información que le concierne. Sin embargo, es fácilmente reconocible que se trata de instrumentos diferentes. El derecho a la información responde a la obligación de los profesionales sanitarios de mantener informado en todo momento al paciente sobre su estado de salud y los tratamientos que se le aplican. Se trata de una información continuada[3230]. La propia jurisprudencia ha señalado que en el derecho a la información la información ha de ser "*puntual, correcta, veraz, leal, continuada, precisa y exhaustiva*"[3231]. El derecho a ser informado reconocido en la normativa sanitaria lo ejercen los pacientes que van a ser sometidos a un tratamiento. Se dirige, la mayoría de veces, a asegurar que éste dé un consentimiento informado sobre determinado tratamiento o a que conozca cómo se desarrolla

---

persona tiene derecho a que se respete su voluntad de no ser informada. La información, que como regla general se proporcionará verbalmente dejando constancia en la historia clínica, comprende, como mínimo, la finalidad y la naturaleza de cada intervención, sus riesgos y sus consecuencias; 2. La información clínica forma parte de todas las actuaciones asistenciales, será verdadera, se comunicará al paciente de forma comprensible y adecuada a sus necesidades y le ayudará a tomar decisiones de acuerdo con su propia y libre voluntad; 3. El médico responsable del paciente le garantizará el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle".

[3226] Artículo 4.3 LBAP: "*El médico responsable del paciente le garantiza el cumplimiento de su derecho a la información. Los profesionales que le atiendan durante el proceso asistencial o le apliquen una técnica o un procedimiento concreto también serán responsables de informarle*". DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 38: el responsable de informar es el profesional sanitario: médico, enfermero… En este sentido se recomienda la realización de cursos formativos para estos sujetos en este sentido.

[3227] Artículo 5.4 LBAP: "*El derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la faculta del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. Llegado este caso, el médico dejará constancia razonada de las circunstancias en la historia clínica y comunicará su decisión a las personas vinculadas al paciente por razones familiares o de hecho*".

[3228] Artículo 7.2 Decreto 272/1986, 25 de noviembre, por el que se regula el Uso de la Historia Clínica de los Centros Hospitalarios en la CAPV; Artículos 2 y 3 Ley 21/2000, 29 de diciembre, de Cataluña, sobre los Derechos de Información concernientes a la Salud y la Autonomía del Paciente, y la Documentación Clínica; Artículo 7 Ley 3/2005, 7 de marzo, de Galicia, de modificación de la Ley 3/2001, 28 de mayo, reguladora del Consentimiento Informado y de la Historia Clínica de los Pacientes.

[3229] STSJ de Cantabria 16 de mayo de 2001, FJ 5: Por otro lado señala, basándose en la LGS, que "el derecho a la información presente una multiplicidad de facetas, que se concentra, en primer lugar en la información acerca del estado de salud del paciente, con extensión al diagnóstico y al pronóstico, esto es cuál es el mal que padece y su gravedad, que es lo primero que un paciente desea saber, dentro de éste capítulo también se comprende la necesaria para tener al corriente al enfermo de las evolución de su mal una vez iniciado el tratamiento". Esta definición se correspondería más con lo que señala la LBAP en el artículo 4 en relación al derecho a la información. El derecho de acceso, parece una facultad más amplia a hacerse con la información concerniente a cada uno.

[3230] MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, pp. 62-63, señala que la obligación de informar es una "obligación de tracto sucesivo".

[3231] STS 29 de mayo de 2003, FJ 1.

una enfermedad concreta que está siendo tratada[3232]. Mientras tanto, el derecho de acceso responde a la facultad del usuario de conocer en un momento determinado el contenido de la historia clínica y demás documentación que contenga datos de carácter personal[3233]. Cualquier usuario, más allá de los pacientes que son sometidos a tratamiento médico en un determinado momento, tiene derecho a conocer lo que en un sistema sanitario determinado se realiza con la información que le concierne.

Se puede observar que en el ámbito sanitario el punto de partida lo constituye el reconocimiento de diferentes instrumentos que posibilitan que el paciente cuente con amplia información, cuando menos sobre los datos que conciernen a su salud. Siendo paciente, a través del ejercicio del derecho a la información se estará constantemente informado sobre su estado. En relación a este tipo de datos la norma general será la información y la excepción la falta de ella[3234]. Las excepciones las constituyen la voluntad del propio paciente de no ser informado y motivos vinculados a la protección de su salud. Con respecto a los demás datos, que no se refieren a su estado de salud, el paciente ejercerá el derecho de acceso siguiendo la regulación establecida en la normativa de protección de datos y la normativa sanitaria. No se tratará, en este último caso, de una información continua, sino del ejercicio puntual del derecho de acceso.

Cuando se es mero usuario, no paciente, cuyos datos constan en el sistema de información de un centro, el conocimiento de los datos y tratamientos que se realizan sobre los mismos se llevará a cabo en todo caso mediante el derecho de acceso. Es cierto que la normativa sanitaria, cuando regula el acceso a la historia clínica se refiere constantemente al paciente[3235] y no al usuario, sin embargo, esto no puede llevar a afirmar que el usuario, cuando no está siendo sometido a un tratamiento médico no es titular del derecho de acceso. Evidentemente, esta interpretación atentaría contra el derecho de acceso genéricamente reconocido en la normativa de protección de datos[3236].

Interesa aquí el análisis del derecho de acceso ejercido sobre los ficheros sanitarios, principalmente sobre la historia clínica. No obstante, el estudio de este derecho deberá recoger en determinados momentos referencias a la institución del derecho a ser informado, pues ambos se encuentran estrechamente relacionados. En ocasiones la regulación sobre este último ayudará a interpretar el régimen jurídico del derecho de acceso.

[3232] Artículo 8 LBAP: "*1. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez que, recibida la información prevista en el artículo 4, haya valorado las opciones propias del caso*". MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 37.

[3233] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 26, señala que cuando en la LBAP se habla del derecho a la información, se está haciendo referencia a la información referida a los parámetros necesarios para que el paciente pueda consentir un tratamiento sanitario determinado. Sin embargo, este derecho se presenta con autonomía propia, como derecho a conocer el estado de salud propio, "en términos adecuados, comprensibles y suficientes".

[3234] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 228, subraya el carácter obligatorio de que los profesionales sanitarios informen con continuidad al paciente sobre los diferentes aspectos de su tratamiento.

[3235] Se define este concepto como "persona que padece física y corporalmente, y especialmente quien se halla bajo atención médica" o como "persona que es o va a ser reconocida médicamente", en http://www.rae.es

[3236] En este sentido el artículo 15.1 LBAP dispone que "*(...) Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizaros por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada*". DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, p. 588.

II.2.2. Breves comentarios sobre el ejercicio del acceso en el ámbito sanitario.

El punto de análisis más interesante lo constituye el relativo a los límites impuestos en la normativa sanitaria al derecho de acceso a la historia clínica. No obstante, merece la pena señalar algunos aspectos sobre cómo se ejerce dicho derecho. La regulación de cómo ha de proceder el titular de los datos a la hora de acceder a la documentación sanitaria debería preverse en la normativa sanitaria, sin embargo, la LBAP no recoge un procedimiento determinado al respecto y dispone que serán los centros los que lo concreten[3237]. En determinados casos se ha producido el desarrollo normativo de este precepto; así la Circular que en la Comunidad de Castilla-La Mancha regula el acceso a la historia clínica[3238], no obstante, se trata de una situación excepcional.

A falta de la normativa concreta que regule estos aspectos, se entiende que será de aplicación la normativa de protección de datos. Prueba de ello es que si se acude a protocolos de actuación que regulan la materia de protección de datos en diferentes sistemas sanitarios se observará que se aplica rigurosamente la normativa general de protección de datos[3239]. En la misma línea, no hay que olvidar las numerosas remisiones que en la LBAP se hacen a esta normativa, incluso en materia de acceso. La propia AEPD a la hora de resolver diferentes cuestiones relativas al acceso sobre la historia clínica se refiere y aplica en muchas ocasiones conjuntamente la LOPD y la LBAP[3240]. Así lo ha hecho también la doctrina más reciente[3241].

Cuando se trata del ejercicio del derecho a la información asistencial que reconoce la LBAP no se prevé un procedimiento especialmente riguroso para llevarlo a cabo. Evidentemente, cuando se es paciente y se está siendo sometido a un tratamiento médico, el derecho de información relativa a la salud de cada uno no deberá someterse a procedimientos férreos o estáticos, sino que debe admitirse una gran flexibilidad en su ejercicio. Hay que tener en cuenta que este derecho a la información está vinculado directamente con la protección de la salud de las personas. Esta finalidad hará que la obligación de los profesionales sanitarios de dar una información continua a los pacientes no deba sujetarse a formalidades rigurosas. Esta idea viene reforzada por el hecho de que se trata de una información que se otorgará verbalmente a los pacientes[3242].

Por el contrario, quien quiera ejercer el derecho de acceso deberá atender al procedimiento pertinente. Como usuario del sistema, o cuando se es paciente y se quiere acceder a datos que van más allá de la pura información asistencial, deberá seguirse un procedimiento determinado.

[3237] Artículo 18.1 LBAP.

[3238] Resolución de 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam (Servicio de Salud de Castilla-La Mancha).

[3239] Instrucción 6/2003, Director General de Osakidetza, 2 de septiembre de 2003, sobre las funciones y obligaciones del personal de Osakidetza con relación a la protección de datos de carácter personal; Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA), aprobado el 27 de diciembre de 2004 y modificado el 29 de diciembre de 2009.

[3240] Resolución AEPD R/00608/2008, 2 de junio de 2008, procedimiento TD/00067/2008.

[3241] RAMÍREZ REYNA, "Accesos legítimos…", cit., 2009, p. 292.

[3242] Artículo 4.1 LBAP.

Sujetarse a una serie de formalidades será necesario por cuanto así se garantiza que el acceso, al igual que la rectificación o la cancelación, se produce dentro de un marco seguro y controlable. La necesidad de acreditar la titularidad de los datos, o la representación, la obligación del responsable de contestar a las solicitudes en un plazo, etc. constituyen elementos que aseguran que los derechos se ejercitarán de manera adecuada.

En relación al ejercicio de este acceso, más allá del procedimiento común ya descrito, merece la pena realizar algún comentario. A) En primer lugar, hay que tener en cuenta que el acceso a la documentación sanitaria plantea el problema de que se trata de una información especialmente técnica[3243]. Tal como se ha dicho al analizar el procedimiento a seguir en el ejercicio del derecho, hay diversas vías para hacerlo efectivo. La normativa sanitaria, cuando se refiere al derecho a la información, exige que la información se dé de manera comprensible para el paciente[3244]. Es recomendable, por lo tanto, que de las diversas formas que se prevén en las normas para hacer efectivo el derecho de acceso se opte por aquéllas que hagan más fácil una colaboración entre el responsable del fichero y el titular de los datos que ayuden a favorecer la comprensión de la información.

B) En segundo lugar, cabe preguntarse por el alcance del derecho al acceso en este ámbito. Más allá de los límites previstos por la normativa de protección de datos y de los límites fijados por la normativa sanitaria cabe preguntarse hasta dónde llega el derecho de acceso. Alguna decisión de la AEPD ha reconocido que el derecho de acceso a la historia clínica abarca todo el contenido reconocido en el artículo 15 LBAP[3245]. Sin embargo, hay que subrayar que el derecho de acceso no se agota con el acceso a esa información. El genérico derecho de acceso puede ejercerse sobre todo fichero que cuente con datos de carácter personal, más allá de las historias clínicas. La jurisprudencia ha matizado que el derecho de acceso no reconoce la facultad de acceder a las muestras biológicas de las que deriva la información, sino sólo a la información[3246]. Dejando a un lado este dato, la facultad se puede ejercer sobre cualquier dato de carácter personal obrante en un sistema sanitario.

C) En tercer lugar, hay que plantear si en el ámbito sanitario es aplicable el limite temporal que establece la normativa de protección de datos al ejercicio del derecho que se analiza. La LBAP no dice nada sobre el límite de 12 meses al regular el acceso a las historias clínicas. En alguna norma interna que regula el acceso a la historia, por el contrario, sí se hace referencia a la

[3243] DE MIGUEL SÁNCHEZ, *Secreto médico…,* cit., 2002, p. 177: señala la preocupación porque el paciente no sea capaz de comprender la información a la que accede.

[3244] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 31: cuando la LBAP señala que la información será comprensible se refiere a que deberá adaptarse al nivel intelectual del receptor, de forma que el nivel técnico deberá acentuarse o relajarse dependiendo del paciente.

[3245] Resolución AEPD R/00608/2008, 2 de junio de 2008, procedimiento TD/00067/2008: cuando se reconoce el derecho de acceso a la HC se refiere al acceso a la información contenida en el artículo 15 LBAP. En algún caso la agencia ha reconocido que no se ha ejecutado este derecho de forma correcta por no haber remitido toda la información a la que se refiere este precepto.

[3246] STSJ de Cantabria 16 de mayo de 2001, FJ 5: en relación al derecho de acceso a la información sanitaria de un paciente, viene a concluir que una cosa es el derecho de acceso, que abarca la información clínica, y otra el acceso a muestras de tejido preparadas para realizar una prueba médica. Evidentemente, el derecho de acceso no abarca este punto.

misma[3247]. En otras, simplemente se acoge la normativa de protección de datos, recogiendo también este punto[3248]. En este sentido, en el ámbito de Osakidetza, se ha señalado en alguna ocasión que "por regla general, el ejercicio del derecho de acceso por intervalos inferiores a los doce meses existe en el caso de que se acredite por el interesado la existencia de indicios que le hacen sospechar de que los datos que se someten a tratamiento son más que los que conoce en virtud del acceso ejercido"[3249]. A pesar de haberse criticado aquí la redacción de la LOPD al respecto, parece lógico pensar que de inicio los mismos motivos que justificaban la adopción de la medida en la normativa de protección de datos existirán en el ámbito sanitario, por lo que deberá entenderse aplicable, también aquí, esta previsión. Sin embargo, hay que volver a apuntar el matiz que antes se ha indicado. Si bien es cierto que una constante solicitud de acceso por los titulares de los datos podría llegar a bloquear los servicios sanitarios, lo cierto es que el criterio para aprobar o denegar el acceso a la documentación sanitaria debería de ser más flexible al apuntado en la LOPD, y lo que debería de justificarse es la denegación por el responsable del fichero y no el acceso, invirtiendo la carga de prueba.

D) Por último, la aplicación de la normativa de protección de datos al ámbito sanitario genera un problema de interpretación que merece ser citado. La LOPD dispone que el afectado tiene derecho a obtener la información que solicita a través de una copia[3250]. De esta regulación podía deducirse que tiene derecho a una copia de la documentación sanitaria, por ejemplo, de la historia clínica. Esta interpretación aparece reforzada por la LBAP, que recoge el derecho del paciente a acceder a la documentación clínica y a obtener una copia de los datos que aparecen en la historia, si bien con los límites que se citarán en relación a los datos de terceros y las valoraciones y opiniones del profesional sanitario[3251]. Es cierto que no se recoge expresamente, como se hacía en normativa sanitaria ya derogada, el derecho a obtener copia de la historia clínica[3252], pero este derecho podría deducirse de la previsión de la LBAP. La jurisprudencia ha llegado a reconocer el derecho a obtener una copia de la historia clínica. En supuestos anteriores a la entrada en vigor de la LBAP se ha llegado a admitir la obligación de los organismos públicos de facilitar a los usuarios o pacientes las historias propias en su integridad[3253]. Con la entrada en vigor de la citada Ley los tribunales han seguido admitiendo el derecho a obtener una copia, si

[3247] Artículo 4.1.d) Resolución de 27 de febrero de 2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam (Servicio de Salud de Castilla-La Mancha).

[3248] Instrucción 6/2003, Director General de Osakidetza, 2 de septiembre de 2003, sobre las funciones y obligaciones del personal de Osakidetza con relación a la protección de datos de carácter personal; Código Tipo de la Asociación Catalana de Recursos Asistenciales (ACRA), aprobado el 27 de diciembre de 2004 y modificado el 29 de diciembre de 2009.

[3249] Informe sobre Adecuación de Determinados Aspectos de la Ley Orgánica de Protección de Datos de Carácter Personal al Proyecto Osabide, complementario a la exposición que el Consejero de Sanidad realizó ante la Comisión de Sanidad del Parlamento Vasco el 23 de mayo de 2002, a fin de dar cuenta del proceso de centralización de los datos de los pacientes recogidos en los centros de salud de Osakidetza.

[3250] Artículo 15.2 LOPD.

[3251] Artículo 18.1 LBAP.

[3252] Punto quinto del Anexo I RD 63/1995, 20 enero de 1995, Ordenación de Prestaciones Sanitarias del Sistema Nacional de Salud: "*Servicios de Información y Documentación Sanitaria.*
Constituyen servicios en materia de información y documentación sanitaria y asistencia:
6. La comunicación o entrega, a petición del interesado, de un ejemplar de su historia clínica o de determinados datos contenidos en la misma, sin perjuicio de la obligación de su conservación en el centro sanitario".

[3253] STSJ País Vasco, 13 diciembre de 1996, FJ 3.

bien excluyendo de su contenido las anotaciones subjetivas del profesional sanitario y los datos referentes a terceras personas que podrían encontrarse, pero incluyendo pruebas como radiografías, TAC, etc.[3254] El TEDH también parece abrir las puertas al derecho de los pacientes a obtener copia de sus datos sanitarios, si bien hace un llamamiento a la importancia de regular con detalle el derecho de acceso a los datos sanitarios[3255].

El derecho a la copia de la historia clínica que se podría deducir de estas consideraciones ha de reinterpretarse. La doctrina ha considerado que de la redacción de la LBAP puede deducirse la voluntad del legislador de entender el derecho a una copia de la historia en un sentido más restrictivo al expuesto hasta ahora[3256]. De esta interpretación resultaría que el paciente tendría derecho a los datos contenidos en la historia, pero no a un ejemplar completo de la misma, salvo en casos puntuales como es el traslado a otro centro o cambio de médico, supuestos que hoy día, con las nuevas tecnologías, tampoco exigen el traslado al paciente de dicha documentación por cuanto la transmisión de la historia podría realizarse a través de medios telemáticos[3257]. El derecho a obtener una copia podría chocar con distintos intereses. Primero, hay que tener en cuenta los límites que la normativa impone al derecho de acceso a la historia clínica que se analizarán en los apartados siguientes[3258]. Y segundo, que el derecho a recibir la copia de toda la historia clínica podría plantear problemas prácticos, pues podría entenderse, como lo ha hecho la jurisprudencia, como derecho del paciente no ya a los datos sino a las pruebas de las que se derivan los datos (radiografías, resonancias, escáner...), cosa que en la práctica sería muy costoso en todos los sentidos. Si bien es cierto que el derecho a la entrega del informe de alta no es suficiente para satisfacer el derecho de acceso[3259], lo cierto es que un derecho generalizado a una copia de la historia clínica sería complicado de llevar a la práctica.

Con esta interpretación no se está diciendo que el titular de los datos no tenga derecho a obtener en determinados casos la copia de la historia clínica. Sin embargo, resulta difícil aceptar una facultad general y común a que cuando quiera se le otorgue dicha documentación. El derecho de acceso puede ejercerse a través de diversas vías. Una de ellas es la obtención de una copia de los datos. El derecho a la copia podría interpretarse en un sentido restrictivo según el cual la obtención de la copia podría darse no siempre que quisiera el titular, sino cuando existiera una causa que justificara el empleo de dicha vía para el acceso y no otra menos costosa

[3254] STSJ de Castilla y León, 29 de mayo de 2007, FJ 8: se analiza el derecho de acceso de un paciente a su historia clínica, apelando a una interpretación amplia de dicho derecho: "En consecuencia y de conformidad con la legislación vigente a la fecha de los hechos litigiosos, el actor tiene derecho a que se le entregue copia de su historia clínica completa que excluya las anotaciones atinentes a la intimidad de terceras personas que consten en ella, así como las anotaciones subjetivas efectuadas por los profesionales que la han elaborado, y que incluya las pruebas diagnósticas practicadas, tales como radiografías, TAC, gammografías y similares (y no sólo los informes sobre tales pruebas) en la medida en que puedan ser reproducidas".

[3255] STEDH 28 de abril de 2009, K. H. y otros v. Eslovaquia, FFJJ 44-58.

[3256] ATELA BILBAO y GARAY ISASI, "Ley 41/2002...", cit., 2004, pp. 72-73.

[3257] DE MIGUEL SÁNCHEZ, *Secreto Médico…*, cit., 2002, p. 180: "en este caso debe prevalecer el derecho a la salud del paciente y remitirse copia íntegra de la HC al centro o médico correspondientes, ya que los elementos subjetivos del facultativo precedente pueden ser de gran interés para el cuidado del enfermo, debiendo los receptores hacer uso reservado de estos componentes subjetivos".

[3258] CRIADO DEL RIO, *Aspectos médico-legales…,* cit., 1999, p. 80.

[3259] FERNÁNDEZ HIERRO, "Régimen jurídico…", cit., 2002, p. 120: el derecho de acceso no se completa con la entrega del informe de alta a un paciente, sino que tiene que tener derecho a acceder a la historia clínica.

como es, por ejemplo, la visualización. Podría plantearse como solución que el titular pagara una tasa por hacerse con esa copia, cuando no existiera una causa determinada que justificara en el caso concreto la solicitud de la copia. En definitiva, habría que atender a cada caso para determinar si el derecho a obtener una copia puede hacerse efectivo, y con qué alcance. Dependiendo del interés que motivara la solicitud de la copia se podría hacer efectiva la misma.

II.2.3. Los límites al derecho de acceso en el ámbito sanitario.

Una vez se ha reconocido la posibilidad de ejercer el derecho de acceso en el ámbito sanitario, es necesario atender ahora a los límites que se le imponen en las normas. Primero se analizarán brevemente los problemas que plantea la aplicación de los límites previstos por la normativa de protección de datos en el ámbito sanitario, para estudiar después los límites que la normativa sanitaria impone al ejercicio de esta facultad.

II.2.3.A. Breve referencia a la aplicación en el ámbito sanitario de los límites dispuestos en la normativa de protección de datos al derecho de acceso.

Se ha visto más arriba que la normativa de protección de datos prevé una serie de límites comunes a los derechos, fundamentalmente, de acceso, cancelación y rectificación. Estas excepciones tienen aplicación en el ámbito sanitario y han de ser tomadas en consideración cuando el titular de unos datos pretende ejercer estos derechos sobre la información sanitaria que le concierne. La recomendación del Consejo de Europa sobre protección de datos médicos trae al sector sanitario estas excepciones que tanto en la Directiva como en la LOPD se recogen. Lo que ahora se analice será de aplicación tanto para el derecho de acceso como para los de cancelación o rectificación. Sin embargo, estas excepciones se estudian aquí debido a que la limitación de la cancelación y la rectificación plantea problemas de mayor envergadura, más allá de estos concretos supuestos. En todo caso, este análisis será breve, debido a que los aspectos más relevantes han sido ya tratados al estudiar los aspectos comunes a los derechos de las personas.

La solicitud de acceso podrá ser rechazada si constituye una medida necesaria para proteger la seguridad del Estado, la defensa o la seguridad pública, o para reprimir los crímenes[3260]. Además, la normativa interna recoge la posibilidad de limitar los derechos de acceso, rectificación o cancelación si se demuestra que el ejercicio de dichos derechos pudiera poner en riesgo determinadas investigaciones. Como se ha dicho, parece que se esté refiriendo la norma a investigaciones de carácter penal, tal y como lo hace la norma europea. Los conceptos empleados, si bien tienen un marcado carácter indeterminado, se refieren sin duda a bienes jurídicos con entidad suficiente para justificar la limitación a la facultad que se comenta. Sin embargo, se está de acuerdo con la doctrina cuando se subraya que cuesta imaginar una situación de riesgo, en la que se entienda necesario excepcionar el derecho al acceso de un paciente a su historia clínica alegando estas excepciones. No se imagina cómo puede afectar

[3260] Artículo 8.2.a) R (97) 5; Artículo 13.1.a), b) y c) Directiva 95/46/CE; Artículo 23.1 LOPD.

ese acceso a la seguridad del Estado, por ejemplo[3261]. Podría pensarse, quizás, en el supuesto en que se quiere evitar que el interesado conozca que su afección deriva de una enfermedad pandémica, debido a que dicho conocimiento pudiera llevar a una situación de alarma, en caso de que el interesado sacara a la luz la citada situación.

La normativa internacional reconoce también la posibilidad de limitar el derecho de acceso cuando el tratamiento de los datos a los que se quiere acceder tiene como fin la investigación científica o la estadística y se confirma que dicho tratamiento no pone en riesgo la intimidad del titular de los datos[3262]. Como se dijera más arriba, lo cierto es que no se entiende aquí el sentido de esta excepción. Parece deducirse que el hecho de que el tratamiento de datos que se pueda estar realizando en dichas investigaciones no afecte a la intimidad justifica la excepción. A esta previsión pueden hacérsele varias críticas. Por un lado, es cuestionable el que se reconozca que la limitación puede realizarse en todos los casos en que se esté llevando a cabo una investigación. Parece que la excepción se aplicará independientemente de las características que tenga la investigación científica: sea de interés privado o general, se refiera a una cuestión de gran relevancia o no, etc. Por otro, no se entiende la razón de ser de esta excepción, pues no se imagina en qué puede perjudicar a la realización de investigaciones o estadísticas el acceso del titular de los datos a la información que le corresponde.

II.2.3.B. Los límites al derecho de acceso recogidos en la normativa sanitaria. Referencia a los supuestos en que el acceso afecta a la confidencialidad de los datos de terceros y la protección de la salud del titular de los datos.

Cuestión importante en el análisis del derecho de acceso en el ámbito sanitario lo ha constituido en muchas ocasiones el eterno debate generado en torno a la propiedad de la historia clínica[3263]. Son muchos los argumentos que se esgrimen desde la doctrina a favor de la titularidad del médico, del paciente o del centro sanitario. Incluso los tribunales[3264] y las normas[3265] se han decantado en algún caso por afirmar la propiedad de alguno de los agentes

[3261] SÁNCHEZ CARAZO, *La Intimidad...*, cit., 2000, p. 147: "de todas formas, si existiese alguna circunstancia que lo justificase, tendría que ser por un tiempo limitado y nunca con carácter indefinido". STEDH 20 de enero de 2009, Uslu v. Turquía, FFJJ 26 y 27, en la que el Tribunal advierte que en este caso el acceso a unos datos médicos concretos no afectan a la seguridad o el orden público, poniendo de manifiesto la dificultad de alegar estos bienes jurídicos con el fin de limitar el derecho de acceso.

[3262] Artículo 8.2.d) R (97) 5; Artículo 13.2 Directiva 95/46/CE.

[3263] SÁNCHEZ CARO y SÁNCHEZ CARO, *El médico y la intimidad…,* cit., 2001, p. 125; DE MIGUEL SÁNCHEZ, *Secreto Médico…*, cit., 2002, pp. 165-173; FERNÁNDEZ HIERRO, "Régimen jurídico…", cit., 2002, p. 112; SAMPRÓN LÓPEZ, *Los Derechos del Paciente…,* cit., 2002, p. 57; MORO AGUADO y TEJEDOR MUÑOZ, *La Historia Clínica...,* cit., 2003, pp. 199-201; RODRÍGUEZ LÓPEZ, *La Autonomía…,* cit., 2005, p. 191; CODÓN HERRERA, "La historia clínica…", 2004, p. 137; MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 169; GÓMEZ PIQUERAS, "La historia clínica…", cit., 2009, p. 129.

[3264] SAP de Barcelona 25 de abril de 2003, FJ 2, en la que se afirma que la historia clínica no es sólo del paciente y que puede servir, como en este caso, como medio de defensa en un proceso penal para defender a un profesional sanitario; SAP de Pontevedra 23 de julio de 2010, FJ 4, donde, más allá de discutir sobre la propiedad de la historia clínica, se llega a la conclusión de que en la mayoría de casos los centros son los responsables máximos de lo que sucede con estos documentos.

[3265] Artículo 18.1 Ley 3/2001, 28 de mayo, de Galicia, reguladora del consentimiento informado y de la historia clínica de los pacientes: "*Las historias clínicas son documentos confidenciales propiedad de las Administraciones sanitarias o entidad titular del centro sanitario cuando el médico trabaje por cuenta y bajo la dependencia de una institución*

implicados sobre la historia clínica. Se entiende aquí que el análisis del derecho de acceso no ha de centrarse en la determinación de la propiedad sobre la historia clínica. Primero, porque tomadas en consideración las diferentes posturas, lo cierto es que todas ellas parten de argumentos válidos. Y, segundo, porque se comparte aquí la idea señalada por parte de la doctrina de que el término propiedad tiene rasgos marcadamente patrimonialistas[3266], que nada tienen que ver con lo que una historia clínica significa. Este carácter patrimonialista se ha dejado ver en textos que han reconocido expresamente el derecho de propiedad de alguno de los agentes sobre la historia clínica, pareciendo llegar a otorgar un derecho absoluto, prácticamente ilimitado sobre el documento[3267].

Este tipo de argumentos no hacen más que distorsionar el conflicto entre los diferentes derechos, pues parecen dar primacía absoluta e ilimitada a uno de los agentes citados a la hora de decidir sobre los documentos sanitarios. Hay que recordar que no existe derecho absoluto alguno, sino que los bienes jurídicos chocan entre sí. Esta realidad hace difícil que se pueda hablar de propiedad, en sentido estricto, cuando se hace referencia a la historia clínica. Partiendo de esta idea, se entiende aquí que el punto de partida ha de ser el reconocimiento de un amplio derecho de acceso al titular de los datos, pero teniendo en consideración otros derechos o intereses con los que colisiona[3268]. El debate debe centrarse en los intereses que los diferentes actores tienen sobre la información que dicho documento contiene[3269]. A pesar de que algún autor haya considerado este planteamiento como una "desviación del problema"[3270], se interpreta que es más práctico fijar el debate en torno al derecho de acceso del paciente sobre la historia clínica y en sus posibles limitaciones, que en la interminable discusión relacionada con el derecho de propiedad sobre este fichero. Así lo ha hecho también la LBAP, al centrarse más en la resolución de las diferentes colisiones que se pueden dar en el ámbito sanitario entre distintos intereses[3271].

Los principales puntos de duda en el análisis del régimen jurídico del derecho de acceso en el ámbito sanitario surgen a la hora de atender a las limitaciones previstas a este derecho. Estos límites son los recogidos en la normativa de protección de datos y en la normativa sanitaria.

---

sanitaria. En caso contrario, la propiedad corresponde al médico que realiza la atención sanitaria". En el mismo sentido, Artículo 23 Ley 1/2003, 28 de enero, de Derechos e Información al Paciente de la Comunidad Valenciana.

[3266] SEOANE RODRÍGUEZ, "¿A quién pertenece...", cit., 2002, p. 250; RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente...,* cit., 2005, p. 194.

[3267] Manifiesto en Defensa de la Confidencialidad y el Secreto Médico, de junio del 2003, que reconoce que "los datos médicos pertenecen a cada paciente, y éste tiene todos los derechos sobre los mismos (...)"

[3268] MÉJICA, "Hacia un Estatuto...", cit., 2002: "es muy fácil decir que el paciente tiene un derecho de acceso absoluto, porque es un derecho que forma parte del núcleo duro del derecho a la intimidad. Yo creo, sin embargo, que es un derecho que hemos de madurar. Así, puede haber partes de la historia que se refieren a la gestión y que pertenecen al hospital; elementos que pueden corresponder al médico o a terceros; también puede encerrar un interés científico, estadístico, docente, etc.".

"Considero que el paciente tiene un derecho de acceso íntegro a la historia clínica, pero con tres limitaciones: las anotaciones personales del médico; la confidencialidad de los datos de terceras personas, y por interés terapéutico del propio paciente".

[3269] AYERA LAZCANO, "Regulación General...", cit., 2003, p. 33: se refiere a la idea de que "es más acertado hablar de titularidad de derechos fundamentales; MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 181.

[3270] DE ANGEL YAGÜEZ, "Problemática de la Historia...", cit., 1997, p. 113.

[3271] DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, 506.

A) Entrando a analizar los límites de manera individual, la LBAP limita el acceso, en primer lugar, cuando afecta a la confidencialidad de los datos de terceros[3272]. La recomendación del Consejo de Europa se pronuncia también, en este sentido[3273]. La LOPD señala como límite al derecho de acceso, cancelación y rectificación la defensa de los derechos de terceros, entre los que se encuentra, el derecho a la confidencialidad sobre los datos de un tercero[3274]. Por su parte, la AEPD ha inadmitido en alguna ocasión la solicitud de acceso a una historia clínica basándose en el argumento de la protección de los datos de un tercero[3275].

Un caso paradigmático de este supuesto lo constituiría el acceso por parte de una persona a sus datos genéticos, que, por las características de dicha información, podrían dar a conocer información sobre el estado de salud de familiares consanguíneos[3276]. En estos casos, parece lógico que el derecho de acceso de una persona no pueda comprometer la intimidad de otras, aunque sean familiares, pues lo contrario podría suponer, incluso, que esas terceras personas no quisieran facilitar dicha información. En todo caso, la limitación basada en la defensa de derechos de terceros ha de contar también con excepciones. Evidentemente, si el tercero otorga su consentimiento no habrá problema alguno para que el acceso pueda producirse[3277]. Pero más allá de este supuesto, cabe pensar que en los casos en que el acceso del interesado se basa en bienes jurídicos de especial relevancia, como puede ser la protección de su salud, el interés del tercero ha de verse superado por el interés legítimo de quien ejerce el acceso[3278].

B) Un segundo límite que reconoce el ordenamiento al derecho de acceso es el de la protección de la propia salud del paciente[3279]. El ejercicio de este derecho no puede suponer un perjuicio para el paciente. Así se reconoce expresamente en la recomendación del Consejo de

[3272] Artículo 18.3 LBAP.
[3273] Artículo 8.2.c) R (97) 5.
[3274] Artículo 23.1 LOPD.
[3275] Resolución AEPD R/01311/2009, 25 de mayo de 2009, procedimiento TD/00945/2009: se estima la inadmisión del acceso de una persona a unos datos pues la información solicitada contiene datos referentes a una tercera persona.
[3276] *Working Document on Genetic Data,* del Grupo de Trabajo sobre Protección de Datos del artículo 29 de la Directiva 95/46/CE, 17 de marzo de 2004, recoge el problema que el derecho de acceso de un paciente a datos genéticos puede plantear en lo relativo a la intimidad de los familiares que puede verse comprometida por este acceso. GÓMEZ PIQUERAS, "La historia clínica…", cit., 2009, p. 144.
[3277] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, p. 220: en torno al acceso de un paciente a datos sanitarios de terceros apuntan que "si los datos no se pueden "individualizar", o en la medida que no lo sean, creemos: a- que la recopilación de dichos datos debe estar absolutamente limitada a situaciones de clara necesidad y, si puede preverse, se le informará al paciente de que tales datos pueden tener estas características y que el acceso a ellos podrá estar limitado; b- en el caso de que se realice la recogida y almacenamiento de este tipo de información, debe quedar a salvo el derecho a la intimidad del tercero y, por lo tanto, opinamos que se debe limitar el derecho de acceso. En todo caso, pensamos que debería existir algún mecanismo por el cual el interesado pudiera recabar el consentimiento del tercero o terceros, si esto fuera posible".
[3278] STEDH, 7 de julio de 1989. Caso Gaskin v. Gran Bretaña, recoge el problema que puede llegar a plantearse entre el derecho de acceso de una persona a ficheros que contienen datos de carácter personal que le conciernen y el derecho a la intimidad de terceras personas. De lo expuesto en esta sentencia podemos concluir que hay supuestos en que el derecho a la intimidad de terceras personas no puede frenar el derecho de otras a acceder a ficheros que contienen datos sobre su persona cuando dicho acceso está justificado por un motivo de envergadura.
[3279] ANDÉREZ GONZÁLEZ, "Aspectos legales...", cit., 2003, p. 239: "aun cuando este supuesto no se regula expresamente entre las excepciones al derecho de acceso a la historia clínica, su consideración como tal deriva de la previsión que la Ley 41/2002 contiene de la necesidad terapéutica como excepción al derecho del paciente a la información sobre su proceso asistencial; ya que si en estos casos cabe limitar el derecho del paciente a la información sanitaria, con idéntico motivo debe exceptuarse el acceso a los datos de la historia clínica afectados por dicha reserva".

Europa sobre la protección de los datos médicos[3280]. La Directiva también prevé la posibilidad de limitar el derecho de acceso con el fin de proteger al interesado[3281]. No se reconoce expresamente la salvaguarda de la salud como bien jurídico que justifica dicha limitación. Sin embargo, cabe incluir la salud en este apartado de la norma, por cuanto que la protección del interesado puede integrar sin dificultad la protección de su salud. En el ámbito interno, la LBAP no reconoce este límite en el apartado dedicado a regular el derecho de acceso, lo que ha llevado en algún caso a negar su existencia en este sector[3282], sin embargo, esta norma recoge la posibilidad de limitar el derecho del paciente a conocer la información sobre su salud por motivos terapéuticos, es decir, cuando el acceso a dicha información puede perjudicar su salud, por ejemplo, porque puede afectar el adecuado desarrollo de un tratamiento médico concreto[3283]. Así se ha interpretado también en normativa interna de determinados sistemas sanitarios, reconociendo expresamente la aplicabilidad del motivo terapéutico para limitar el derecho de acceso[3284].

De todas estas consideraciones se ha acabado por asumir generalmente por la doctrina que los motivos terapéuticos pueden justificar el límite al derecho de acceso[3285]. El concepto de "motivos terapéuticos" ha de ser, sin embargo, matizado. Ante la vaguedad de los términos no puede hacerse una interpretación amplia de los mismos, pues ello podría llevar a argumentar el motivo terapéutico continuamente para negar el derecho de acceso, vaciando así de contenido dicho derecho en el ámbito sanitario[3286]. En el caso que ahora se trata entran en juego el derecho de acceso de una persona a la información que consta en los ficheros sanitarios y su derecho a la salud. Chocan dos bienes jurídicos de los que es titular la misma persona: la autonomía o autodeterminación personal, representada en el ejercicio del derecho de acceso, y el derecho a la salud o la integridad del paciente. Se trata de valorar si el hecho de que un paciente conozca los detalles sobre su estado físico o mental puede afectar de alguna manera a su salud. Ante una posible interpretación amplia de la limitación se entiende aquí que el punto de partida en la resolución de esta confrontación hay que situarlo a favor del principio de autonomía, tan reivindicado en los últimos años, y que se concretaría en el respeto al derecho a la información total del paciente[3287]. A partir de este punto se podrían reconocer supuestos claros, atendiendo a criterios científicos, en que el acceso a los datos pone en riesgo la salud del

[3280] Artículo 8.2.b) R (97) 5.
[3281] Artículo 13.1.g) Directiva 95/46/CE.
[3282] NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, p. 196: apunta que el artículo 18.3 LBAP no plantea las razones terapéuticas como motivo de limitar el derecho de acceso a la historia clínica, por lo que el profesional sanitario no podrá denegar el acceso por estas razones.
[3283] Artículo 5.4 LBAP.
[3284] Artículo 3.3 Resolución de 27/02/2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam.
[3285] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 72: señala también que el derecho de acceso puede limitarse por razones terapéuticas.
[3286]DE MIGUEL SÁNCHEZ, *Secreto médico…,* cit., 2002, p. 177; MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, p. 37: reconoce la posibilidad de limitar el acceso por motivos terapéuticos. Sin embargo, este motivo hay que interpretarlo de manera limitada de forma que el punto de partida sea el reconocimiento del derecho de acceso.
[3287] FERNÁNDEZ HIERRO, "Régimen Jurídico...", cit., 2002, p. 123: "Como norma el paciente tiene derecho a la totalidad de su historia clínica".

paciente[3288], y en los que el profesional de la medicina pudiera decidir no otorgar cierta información al paciente. Hay que subrayar que esta limitación se aplicará en casos especialmente claros en que el profesional sanitario no encuentre alternativa al ocultamiento de la información. Se está de acuerdo con la consideración de que el motivo terapéutico podrá limitar este derecho a la información cuando se trate de un mal grave, efectivo, real e inminente[3289]. Se dice esto porque muchas veces basta con dar la información de determinada forma para que no haya necesidad de ocultarla[3290]. Podría plantearse también como opción en los sistemas sanitarios, para un mayor respeto del principio de autonomía, que, siempre que sea posible, antes de iniciar el tratamiento se le indique al paciente si en el caso que se expone desea ser informado sobre cualquier circunstancia, por grave que sea, o si prefiere dejar a criterio médico los límites en el ejercicio del derecho de acceso.

A la hora de aplicar este límite al derecho de acceso, será el médico el que determinará si los motivos terapéuticos se dan, y en qué medida, y quien justificará así la limitación del derecho de acceso[3291]. Podría pensarse que este criterio es paternalista y poco fundamentado[3292]. Sin embargo, parece necesario que en beneficio de la salud del paciente se le reconozca al profesional sanitario cierta facultad para decidir si es conveniente o no que determinada información llegue al conocimiento del paciente, sin que esto tenga que suponer una merma del principio de autonomía que debe regir la relación médico-paciente[3293]. Ya se dijo al analizar el principio de autonomía que éste ha de ser interpretado de manera relativa y no de forma absoluta. Un paternalismo bien entendido y limitado a circunstancias concretas debe tener cabida en la relación médico-paciente. Si se atiende a la especialidad psiquiátrica como ejemplo, puede verse claramente que el acceso a determinados datos de la historia podría resultar traumático y perjudicial para el paciente[3294].

[3288] DE MIGUEL SÁNCHEZ, *Secreto Médico…*, cit., 2002, p. 178: "La propuesta mencionada puede ser una solución adecuada a los casos conflictivos, siempre que se aplique en sus justos términos, es decir, en circunstancias excepcionales y siguiendo un criterio médico que sopese cuidadosamente los pros y contras de dar, en cada caso, una información completa al paciente".

[3289] RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente...,* cit., 2005, p. 103.

[3290] SEOANE PRADO, "Información Clínica...", cit., 1997, pp. 242-244: parece defender la teoría de que hay que informar en todo caso al paciente, siendo lo fundamental la forma de informar.

[3291] Declaración de la Asociación Médica Mundial sobre las Consideraciones Éticas de las Bases de Datos de Salud, octubre 2002, en http://www.wma.net, en el principio nº 11, reconoce que "en circunstancias raras y limitadas, se puede ocultar la información de salud a un paciente, si al revelarla existen muchas posibilidades de un efecto adverso importante para el paciente o para terceros. El médico deberá justificar toda decisión de ocultar información al paciente".

[3292] DE MIGUEL SÁNCHEZ, "Intimidad e Historia...", cit., 2003, p. 29, y C. SÁNCHEZ CARAZO, *La Intimidad...*, cit., 2000, p. 147: "el derecho de autonomía y el de libertad del interesado están por encima del de beneficencia. ¿Tiene alguien derecho a decidir sobre lo que podemos conocer de nosotros mismos?".

[3293] Documento Final del Grupo de Expertos en Información y Documentación Clínica, Madrid, 26 de noviembre de 1997, punto 3.5.c): "Información claramente perjudicial para la salud del paciente. En este supuesto es ineludible la valoración de los valores en conflicto, para lo cual parece recomendable el asesoramiento del Comité Asistencial de Ética. Este requerimiento es especialmente conveniente cuando la situación descrita concurre con el deseo expreso por el paciente de conocer su verdadero estado de salud. Debe hablarse aquí de necesidad terapéutica".

[3294] MORALES PRATS, "Derecho a la Intimidad…", cit., 2001, p. 146: «en el ámbito del tratamiento psiquiátrico de algunas enfermedades, el médico puede proyectar en esa historia clínica que el paciente tiene un mal diagnóstico, o que es bastante irreversible el proceso; y si el paciente quiere acceder a esa historia clínica, habrá que segregar la información que se le facilita porque puede recibir un fuerte impacto emocional".

C) Por último, aunque no pueda considerarse un límite, hay que tener en cuenta también el derecho a no saber, como un supuesto en que el titular de los datos no tiene acceso a la información. Este derecho se podría fundamentar en la autonomía o, como lo ha hecho parte de la doctrina, en el derecho a la intimidad, entendido en un sentido amplio, como capacidad de controlar la información que concierne a cada uno. La posibilidad de acceder a dicha información reconoce también la vertiente negativa del mismo derecho, como facultad de no conocer la información[3295]. La doctrina ha señalado en algún caso que la virtualidad de este derecho se rebaja en la medida en que en la práctica es difícil no querer saber algo que se desconoce[3296]. Sin embargo, es evidente que en el ámbito sanitario no resulta anormal no querer conocer el estado de salud de cada uno, sobre todo, cuando se trata de situaciones de cierta gravedad.

El derecho a no saber no puede observarse como un derecho general a no ser informado o como una posibilidad a renunciar en general al ejercicio del mismo, sino como derecho a no saber en un momento determinado cuál es su estado de salud o el tratamiento que se le debe aplicar[3297]. Este derecho ha de limitarse cuando pone en riesgo la salud del propio paciente o de terceros. Con respecto al primer caso, piénsese en las consecuencias que pudieran derivar de la falta de información en el supuesto de que el paciente pueda adoptar medidas preventivas para hacer frente a una patología determinada[3298]. Respecto al segundo, hay que tener en cuenta, como ejemplo, los casos en que una persona sea portadora de una enfermedad contagiosa. Si no se informa a este sujeto de que es portador de dicha enfermedad el resultado será, como se puede imaginar, nefasto[3299].

II.2.3.C. Especial referencia al límite a acceder a las anotaciones subjetivas realizadas por el profesional sanitario en los documentos sanitarios.

La normativa sanitaria establece un límite al derecho de acceso en los derechos que los profesionales sanitarios puedan tener sobre la información que crean[3300]. Parece que la norma está haciendo referencia a los derechos de propiedad intelectual de los que los profesionales pueden ser titulares sobre las anotaciones subjetivas, valoraciones y demás diagnósticos que puedan hacer partiendo de la información objetiva concerniente al interesado[3301]. Sin embargo, también se ha fundamentado este límite en el derecho a la intimidad de los profesionales sanitarios[3302]. La LOPD no hace mención a esta excepción. Tampoco lo hace el RDLOPD. Este

[3295] REQUEJO NAVEROS, *El Delito de Revelación…,* cit., 2006, p. 290: fundamenta el derecho a no saber en el derecho a la intimidad, entendida en sentido amplio, que incluye también el derecho a la autodeterminación informativa: el control sobre los datos de cada uno justifica que no quiera saber. REQUEJO NAVEROS, "El Derecho a no saber…", cit., 2006, en el mismo sentido.
[3296] NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, pp. 125-126,.
[3297] RODRÍGUEZ LÓPEZ, *La Autonomía…,* cit., 2005, p. 84.
[3298] MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 65.
[3299] DE LORENZO Y MONTERO, *Derechos y Obligaciones…,* cit., 2003, p. 34: la LBAP limita el derecho a no saber en el 9.1, en el que la salud del paciente, el interés de terceros o de la colectividad pueden ser argumento suficiente para justificar la información obligada. Por ejemplo, con la información obligada al paciente se podrían evitar contagios; REQUEJO NAVEROS, *El Delito de Revelación…,* cit., 2006, p. 296; NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, pp. 125-126; DOMÍNGUEZ LUELMO, *Derecho sanitario…,* cit., 2007, 339.
[3300] Artículo 18.3 LBAP.
[3301] MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 210.
[3302] LARIOS RISCO, "La historia clínica…", cit., 2009, p. 174; CANTERO RIVAS, "La historia clínica…", cit., 2009, p. 212.

reglamento dispone que el derecho de acceso se ejerce sobre los datos base del afectado y también sobre la información resultante de cualquier elaboración o proceso informático llevado a cabo sobre dichos datos base[3303]. Podría pensarse que esta información resultante abraza también las valoraciones realizadas sobre los datos objetivos. Sin embargo, no parece que el reglamento se esté refiriendo en este último caso a las valoraciones que de los datos objetivos sobre una persona se puedan realizar, sino a nuevos datos que pudieran derivar, por ejemplo, de la puesta en común de diferentes datos base. La recomendación del Consejo de Europa sobre la protección de datos médicos tampoco abraza esta excepción.

La normativa sobre protección de datos no establece límite alguno al acceso en los datos o anotaciones subjetivas. El acceso se puede ejercer sobre los datos, y estos pueden ser comprendidos de una manera amplia que abarque tanto la información objetiva como la subjetiva. Sin embargo, atendiendo a la normativa sanitaria los tribunales parecen haber realizado una interpretación literal de la LBAP con respecto al derecho de acceso, asumiendo así la virtualidad de este límite[3304]. Así se ha hecho también en alguna decisión de la AEPD, en la que se ha limitado el derecho de acceso a la documentación sanitaria argumentando que esta facultad no abraza el derecho de recabar valoraciones de índole médica o técnica de los profesionales[3305]. Parte de la doctrina ha admitido también este límite[3306]. Más arriba ya se ha comentado someramente el problema que plantean este tipo de informaciones que no son estrictamente objetivas. Corresponde en este momento profundizar en esta cuestión.

El límite al acceso se sitúa en la normativa sanitaria en las "anotaciones subjetivas" que pueda realizar el profesional sanitario sobre los pacientes. Son varias las críticas que se pueden hacer al empleo de este concepto[3307]. El primer problema deriva de la indefinición del concepto anotaciones subjetivas[3308], y es que dicha indefinición podría llevar a una interpretación

[3303] Artículo 29.3 RDLOPD.

[3304] STSJ de Castilla y León, 29 de mayo de 2007, FJ 8: se analiza el derecho de acceso de un paciente a su historia clínica, apelando a una interpretación amplia de dicho derecho: "En consecuencia y de conformidad con la legislación vigente a la fecha de los hechos litigiosos, el actor tiene derecho a que se le entregue copia de su historia clínica completa que excluya las anotaciones atinentes a la intimidad de terceras personas que consten en ella, así como las anotaciones subjetivas efectuadas por los profesionales que la han elaborado, y que incluya las pruebas diagnósticas practicadas, tales como radiografías, TAC, gammografías y similares (y no sólo los informes sobre tales pruebas) en la medida en que puedan ser reproducidas".

[3305] Resolución de la AEPD R/00969/2008, 31 de julio de 2008, procedimiento TD/00320/2008. En algún caso parece haberse limitado el derecho de acceso a la información sanitaria, por exceder lo previsto en la LOPD y reglamento como los datos de base y los resultantes de éstos: "Los datos personales de la interesada que deben ser facilitados en atención al derecho de acceso, son todos aquellos datos relativos a la determinación y constatación de sus lesiones, su evolución y, en su caso, las secuelas advertidas, que afectan a la salud de la titular de los datos, pero no pueden incluirse, como datos de base, las valoraciones o apreciaciones de índole médica sobre el encaje de las lesiones o secuelas padecidas en la aplicación del baremo del Real Decreto Legislativo 8/2004 que deben ser consideradas estimaciones de orden técnico propias de un facultativo médico".

[3306] MARTÍNEZ AGUADO, "Aspectos éticos…", cit., 2002, p. 90: el paciente tiene derecho al acceso de datos objetivos, no a datos subjetivos; SÁNCHEZ CARO, y ABELLÁN, *Datos de salud…,* cit., 2004: p. 54: parecen negar la posibilidad de acceder a los datos subjetivos de la historia: observaciones, teorías, etc. de los profesionales sanitarios.

[3307] SEOANE, HERNANDO ROBLES, DE ASÍS CUBAS y GONZÁLEZ, "Historia clínica y derechos fundamentales…", 2006.

[3308] DÍAZ MÉNDEZ, "Historia clínica…", cit. 2004, p. 316; TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 72; CANTERO RIVAS, "La historia clínica…", cit., 2009, p. 213.

excesivamente amplia de la excepción[3309]. Hay que tener en cuenta que en el ámbito sanitario la gran mayoría de diagnósticos se fundamentan en valoraciones personales del profesional sanitario[3310]. Ni qué decir en campos como la psiquiatría donde la mayoría de la información constituye la valoración del comportamiento del paciente[3311]. Si este tipo de apreciaciones se consideraran anotaciones subjetivas el derecho de acceso quedaría reducido a su mínima expresión. Algunas normas han tratado de dar contenido a este concepto. En algún caso se ha aceptado la consideración de anotación subjetiva "únicamente" de la siguiente información: "*(…) valoraciones sobre hipótesis diagnósticas no demostradas, sospechas acerca de incumplimientos terapéuticos, sospechas de tratamientos no declarados, sospechas de hábitos no reconocidos, sospechas de haber sido víctima de malos tratos y comportamientos insólitos*"[3312]. En algún otro caso se ha dado una definición más genérica, entendiendo por dicho concepto las valoraciones personales, fundadas o no en datos clínicos, que no forman la historia clínica pero que pueden influir en el diagnóstico y tratamiento médico, una vez se hayan constatado[3313]. La jurisprudencia en algún caso ha parecido dar también contenido a este concepto, señalando que se refiere a las "impresiones personales sobre el paciente o su entorno, actitud, comportamiento o relaciones del paciente"[3314]. También la doctrina ha hecho algún matiz al respecto, distinguiendo estas anotaciones de los diagnósticos y pronósticos, y definiéndolos como las impresiones personales del profesional sobre el paciente o su entorno[3315].

[3309] ATELA BILBAO y GARAY ISASI, "Ley 41/2002 de derechos…", cit., 2004, p.50.

[3310] TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 71: "no siempre es fácil distinguir las anotaciones subjetivas de aquella información o juicio clínico que refleja el estado de salud del paciente y que necesariamente tiene que ser subjetivo".

[3311] ATELA BILBAO y GARAY ISASI, "Ley 41/2002 de derechos…", cit., 2004, p.50.

[3312] Artículo 4.3.7.b) Resolución de 27/02/2009, de la Dirección Gerencia, mediante la que se aprueba la Circular 1/2009, sobre uso, acceso, cesión de datos y conservación de la Historia Clínica en el ámbito del Sescam; Artículo 64.4 Ley 17/2010, 8 de noviembre, de derechos y deberes de las personas en materia de salud en la Comunidad Foral de Navarra.

[3313] Artículo 21 Decreto 29/2009, 5 de febrero, de Galicia, por el que se regula el Uso y Acceso a la Historia Clínica Electrónica: "*(...) A los efectos de lo dispuesto en el párrafo anterior se entiende por anotaciones subjetivas las valoraciones personales, sustentadas o no en los datos clínicos de que se disponga en ese momento que no formando parte de l historia clínica actual del/de la paciente o usuario/a, puedan influir en el diagnóstico y futuro tratamiento médico una vez constatadas*". En el mismo sentido artículo 32.4.d) Ley 3/2005, 8 de julio de 2005, de Información Sanitaria y Autonomía del Paciente: "*Anotaciones subjetivas de los profesionales sanitarios. A los efectos de lo dispuesto en esta Ley y en sus disposiciones de desarrollo, se entenderán por anotaciones subjetivas las impresiones de los profesionales sanitarios, basadas en la exclusiva percepción de aquéllos, y que, en todo caso, carecen de trascendencia para el conocimiento veraz y actualizado del estado de salud del paciente, sin que puedan tener la consideración de un diagnóstico*".

[3314] STSJ de Castilla y León, 29 de mayo de 2007, FJ 8: "El tribunal hace una referencia también a lo que puede entenderse por las anotaciones subjetivas que podrían quedar fuera del alcance del derecho de acceso: "tales como, impresiones personales sobre el paciente o su entorno, actitud, comportamiento o reacciones del paciente, etc.), datos éstos que no deben ser entregados (tal y como ya expresamente establece el art. 18.3 de la Ley 41/2002".

[3315] "Historia clínica y derechos fundamentales: una reflexión sobre las anotaciones subjetivas", *Datospersonales.org* nº 21, 2006: La LBAP no define lo que son las anotaciones subjetivas. Según la doctrina las anotaciones "no son los juicios clínicos, sino las anotaciones personales clínicas que se distinguen con mayor o menor claridad de los resultados de las exploraciones, el juicio diagnóstico, el pronóstico y el tratamiento, pues no surgen de la observación de un hecho biológico o de su evolución y no plantea alternativas diagnótiscas o decisiones clínicas; por lo tanto, no forman parte de la historia clínica y, por ende, no pueden ser objeto del derecho de acceso del paciente" Se definen también como "impresiones personales del médico fruto de su labor deductiva sobre el enfermo o su entorno, de carácter inicial en el *iter* de la relación asistencial y que ha de poseer trascendencia clínica; son, por tanto, juicios de valor que no tiene porque conocer el paciente"; CANTERO RIVAS, "La historia clínica…", cit., 2009, p. 214:

Como se puede observar, no es tarea sencilla dar un contenido concreto a estas anotaciones. Además, se plantea el problema práctico de quién ha de ser en cada caso el que determine que en una historia clínica existen valoraciones de este tipo que han de ser salvaguardadas ante el acceso del paciente o usuario. Como se ha repetido en relación a otros supuestos en que se exceptúa este derecho, resulta peligroso otorgar esta facultad al profesional sanitario, en la medida en que, ante la indeterminación de los conceptos, se le estaría otorgando un amplio margen de actuación. Podría plantearse la necesidad de crear un órgano *ad hoc* dirigido a hacer efectivo el derecho de acceso de los usuarios.

Más allá del evidente problema que plantea el distinguir los datos objetivos y los subjetivos en un ámbito como el de la medicina, en el que incluso los datos *a priori* más objetivos pueden ser interpretables[3316], el segundo punto crítico que plantea este límite derivaría de la fundamentación de este límite. Se ha dicho que la protección de las anotaciones subjetivas se basaría en un pretendido derecho a la propiedad intelectual o derecho a la intimidad del profesional sanitario. Es evidente que las opiniones que el profesional sanitario aporta a la historia clínica no pueden considerarse datos puramente objetivos[3317]. Sin embargo, estos argumentos presentan ciertos problemas interpretativos.

A) Interpretar que el paciente no tiene derecho de acceso a estos datos basándose en un supuesto derecho a la propiedad intelectual, cuyo titular es el profesional sanitario no es sencillo. En primer lugar, porque a pesar de que las opiniones del profesional no son datos puramente objetivos, son tratados como tal, pues las decisiones del médico se basarán en estas apreciaciones. Esta circunstancia hace pensar que sobre estos datos subjetivos tiene que recaer el mismo derecho de acceso que recae sobre los datos objetivos. Y en segundo lugar, porque el derecho a la propiedad intelectual que se reclama sobre estas anotaciones no puede admitirse tal y como lo hacen muchos autores, debido a que el reconocimiento del derecho a la propiedad intelectual que sobre una determinada creación realiza la Ley de Propiedad Intelectual se fundamenta en fines que nada tienen que ver con los fines asistenciales que persigue la historia clínica[3318]. Incluso si se aceptara la existencia de un derecho a la propiedad intelectual sobre las anotaciones subjetivas sería dudoso sobre quién recaería la titularidad de este derecho, si sobre el médico o sobre el centro que contrata a dicho profesional[3319]. En todo caso, parece dudoso

"anotaciones subjetivas son aquellas que recogen impresiones del profesional no apoyadas en datos objetivos que carecen de trascendencia para el conocimiento veraz y actual del estado de salud del paciente".

[3316] ATELA BILBAO y GARAY ISASI, "Ley 41/2002...", cit., 2004, p. 50; "Historia clínica y derechos fundamentales: una reflexión sobre las anotaciones subjetivas", *Datospersonales.org* nº 21, 2006: Según el autor, la división entre datos objetivos y subjetivos es una división artificial, pues todo dato es en parte objetivo, valorativo…

[3317] SAP de Alicante 6 de julio de 2001, FJ 3, hace referencia a esta distinción: "La Historia Clínica comprende no sólo datos objetivos, que esos sí deben serle entregados al paciente que lo reclama sobre la atención recibida, sino además datos personales y propios de estudios, hipótesis, impresiones plasmadas en papel, etc., que no pertenecen al paciente sino al profesional que lo atendió".

[3318] LAFARGA i TRAVER, "Problemas legales…", cit., 1999, p. 46: "esta aportación del médico no da lugar a una propiedad intelectual sobre la historia clínica en el sentido jurídico del término por cuanto el derecho de propiedad intelectual tiene unas repercusiones fundamentalmente comerciales, en términos de derechos de autor, por la reproducción, difusión o explotación de los productos de la actividad intelectual u obras de literatura, música, artes gráficas, etc., que no son en absoluto extrapolables a la historia clínica (...)".

[3319] RDL 1/1996, 12 de abril de 1996, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia, artículo 51: "*1. La*

que este pretendido derecho del profesional sanitario pueda llegar a justificar una interpretación amplia del límite a un derecho de acceso, que en última instancia constituye un mecanismo de salvaguarda del derecho a la autodeterminación informativa y el derecho a la salud. Así pues este límite deberá ser interpretado de manera especialmente estricta[3320].

B) La alegación del derecho a la intimidad del profesional sanitario para basar este límite también presenta problemas. Primero, porque argumentar la intimidad del profesional cuando la información se refiere al paciente no hace fácil la aplicabilidad de esta consideración. Y segundo, porque esta consideración abre la puerta a que se realice una interpretación amplia de la intimidad del profesional que posibilitaría una aplicación laxa de la excepción.

C) Si se entendiera la excepción que ahora se analiza en sentido amplio podrían llegar a justificarse situaciones verdaderamente absurdas. Piénsese, por ejemplo, en el caso en que un paciente cambia de médico. Si se aceptara dicha interpretación expansiva podría llegar a interpretarse que el nuevo profesional sanitario que va a atender al paciente no tendrá posibilidad de acceder a la historia completa, teniendo que limitarse dicho acceso a los datos objetivos. Evidentemente, la protección de la salud del paciente sugiere que el nuevo profesional deba tener acceso incluso a las anotaciones subjetivas[3321]. El mismo argumento puede servir para justificar que el propio paciente o titular de los datos deba tener acceso a este tipo de anotaciones, por lo menos cuando la negación de dicho acceso pueda perjudicar su salud.

Se ha comentado como argumento favorable a la aplicación de este límite el hecho de que no aceptar esta excepción al acceso podría hacer que el profesional sanitario cambie la forma de redactar la historia clínica[3322]. En atención a este argumento se ha planteado la posibilidad de crear dos historias clínicas, una conteniendo datos objetivos y la otra los datos subjetivos[3323]. Frente argumentos de esta índole se podría alegar que el ocultamiento al interesado de estos datos subjetivos alteraría la relación médico-paciente al generar cierta desconfianza hacia los

transmisión al empresario de los derechos de explotación de la obra creada en virtud de una relación laboral se regirá por lo pactado en el contrato, debiendo éste realizarse por escrito.
2. A falta de pacto escrito, se presumirá que los derechos de explotación han sido cedidos en exclusiva y con el alcance necesario para el ejercicio de la actividad habitual del empresario en el momento de la entrega de la obra realizada en virtud de dicha relación laboral".

[3320] MURILLO DE LA CUEVA, "El Derecho Fundamental…", cit., 2006, pp. 38-39: las anotaciones subjetivas hay que entenderlas en sentido restrictivo. "es más que discutible que ese interés profesional sea título suficiente para impedir el ejercicio del derecho que estamos examinando".

[3321] DE MIGUEL SÁNCHEZ, *Secreto médico…,* cit., 2002, pp. 179-180: parece que la autora defiende la limitación del acceso a la historia clínica a favor de los derechos de los profesionales sanitarios. Sin embargo, matiza que cuando una persona cambia de médico, el nuevo médico si ha de tener acceso a toda la historia clínica, pues favorece el tratamiento sanitario; MARTÍNEZ AGUADO, "Aspectos éticos…", cit., 2002, p. 91, reconoce este derecho de acceso a las anotaciones subjetivas a los profesionales sanitarios debido a que están sujetos al deber de secreto. Sin embargo, lo limita cuando quien pretende acceder es el propio paciente.

[3322] FERNÁNDEZ HIERRO, "Régimen jurídico…", cit., 2002, p. 122: si se reconociera el derecho a una copia de la HC al paciente podría pasar que los profesionales empezaran a cambiar la forma de escribir dichas historias.

[3323] Código tipo de tratamiento de datos de carácter personal para odontólogos y estomatólogos de España, diciembre 2009: El derecho de acceso se ha de hacer respetando las anotaciones subjetivas de los profesionales sanitarios. Para ello, se señala que estas anotaciones deberán constar de forma separada del resto de datos y demás documentación clínica. DE MIGUEL SÁNCHEZ, *Secreto Médico…*, cit., 2002, p. 179.

profesionales sanitarios que no quieren otorgar esa información[3324]. Esta situación podría afectar en última instancia al tratamiento médico.

Se ha apuntado también como argumento que justifica este límite el hecho de que el acceso a toda la historia clínica podría llevarle a conocer datos que no entiende, que puede malinterpretar, etc[3325]. Sin embargo, ante el hecho cierto de que existan partes o anotaciones que el paciente puede no entender o malinterpretar, la solución no tiene que ser que el paciente no acceda a sus datos, sino que el médico le asista en ese acceso. En este sentido, es significativa la consideración que la Directiva y la recomendación del Consejo de Europa realizan sobre la posibilidad de que los estados dispongan que este acceso se lleve a cabo mediante profesionales sanitarios[3326]. En el ámbito interno esta previsión puede deducirse de la normativa sanitaria, que al referirse al derecho del paciente a conocer la información relativa a su salud y a los tratamientos médicos que se le van a aplicar, dispone que la información será remitida por los profesionales sanitarios que le atiendan[3327].

El límite que ahora se analiza plantea verdaderos problemas, sobre todo porque las anotaciones subjetivas constituyen apuntes muy variados y de diferente consideración. Quizás podría plantearse la solución desde una distinción entre las apreciaciones que el profesional realiza sobre el paciente, y las apreciaciones o anotaciones que no tienen relación directa con el paciente[3328], y que suponen una creación o una teoría o una opinión sobre una situación determinada en abstracto y no a opiniones o teorías aplicadas a un caso o sujeto particular. Partiendo de esta distinción, podría aceptarse un derecho de acceso sobre las primeras y negar este mismo derecho sobre las segundas, teniendo que apuntar el profesional sanitario estas últimas en un apartado distinguido en la historia clínica[3329]. O al igual que ha hecho parte de la doctrina ya citada al dar contenido al concepto de anotaciones subjetivas, podría interpretarse que las anotaciones se limitan a las apreciaciones estrictamente subjetivas realizadas por el profesional sobre aspectos del paciente que nada tienen que ver con el estado de salud de este último, a saber: personalidad, apreciaciones sobre el entorno, entre otros. Sin embargo, ante esta posibilidad cabe realizar dos matizaciones. Primero, teniendo en cuenta el concepto tan amplio que se ha dado sobre los datos de salud, parece difícil que se pueda hablar en el ámbito sanitario sobre información no vinculada a la salud del paciente o usuario. Segundo, incluso entendiendo que se trata de datos no relacionados con la salud de las personas, cabría preguntarse cuál es la finalidad del tratamiento de estos datos sobre la personalidad. La inclusión de estas apreciaciones, que en ocasiones pueden incluso constituir comentarios despectivos de los

[3324] ANTEQUERA VINAGRE, "Historia Clínica...", cit., p. 20.
[3325] CODÓN HERRERA, "La Historia Clínica...", cit., 2004, p. 150: "La historia clínica en manos del paciente se presta a que realice interpretaciones equivocadas de los comentarios expuestos en ella, unas veces por *desconocer la materia*, otras por considerarlos *ofensivos*, y otras por *ser comprometidos* para él".
[3326] Considerando 42 Directiva 95/46/CE; Artículo 8.1 R (97) 5.
[3327] Artículo 4.3 LBAP.
[3328] HERNÁNDEZ MARTÍNEZ-CAMPELLO, "La Ley 41/2002...", cit., 2004, p. 189, recoge, haciendo suyas las palabras de ALMAGRO NOSETE: "Por anotaciones subjetivas debemos entender (...) <<aquellas que recogen impresiones del profesional no apoyadas en datos objetivos que carecen de trascendencia para el conocimiento veraz y actual del estado de salud del paciente>>".
[3329] TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 40 (nota al pie nº 54): "lo adecuado es que el profesional sanitario no incluya las notas subjetivas dentro de la historia clínica".

pacientes o su entorno, debería estar justificada en cada caso. Si no se trata de información relacionada con el estado de salud del paciente o usuario ¿cómo se justificaría su incorporación a la historia clínica? De lo contrario, si se entiende que concierne a la salud, ¿cuál sería el argumento suficiente para limitar el derecho de acceso del titular de dicha información a los datos?[3330]

Se entiende aquí que la virtualidad del límite previsto por la normativa sanitaria ha de ponerse en cuestión. En general, la posibilidad de ocultamiento de las anotaciones subjetivas parece más un privilegio de los profesionales que un derecho de los mismos[3331]. Más allá de teorías dirigidas a la interpretación de la letra de la Ley, se entiende aquí, de acuerdo con un sector doctrinal y atendiendo a todo lo dicho hasta ahora, que el límite que propone la LBAP al derecho de acceso es difícilmente defendible en Derecho. La limitación al acceso ha de venir no de la distinción entre información subjetiva y objetiva, negando el acceso sobre los primeros, sino de la aplicación de criterios estrictamente médicos, independientemente de si los datos son objetivos o subjetivos[3332]. Sea como sea, incluso en el supuesto de que se niegue el acceso del titular de los datos a las anotaciones subjetivas de la historia clínica, deberá informársele al paciente sobre la existencia de esas anotaciones y sobre el hecho mismo de la reserva ejercida sobre éstas[3333].

III. DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN.

III.1. La rectificación y cancelación en la normativa de protección de datos.

Además del derecho de acceso el *habeas data* se compone de otras facultades de especial relevancia. Entre ellas hay que resaltar los derechos de rectificación y cancelación. Se analizará ahora la regulación que la normativa de protección de datos realiza de estos derechos haciendo especial hincapié en su importancia como facultades cuyo correcto ejercicio es indispensable para garantizar la buena calidad de la información.

III.1.1. La importancia de la rectificación y la cancelación como instrumentos para guardar la calidad de los datos.

El respeto a los principios de veracidad, pertinencia y finalidad, como se había expuesto anteriormente, tiene una importancia capital cuando se trata de llevar a cabo cualquier manipulación de datos de carácter personal[3334]. Esta circunstancia se acentúa cuando se está haciendo referencia al ámbito sanitario. En este sector el respeto a los principios de calidad tiene relevancia desde dos vertientes, tanto desde el punto de vista del derecho a la autodeterminación informativa, como del derecho a la protección de la salud. Primero, es evidente que el derecho a

[3330] SEOANE, HERNANDO ROBLES, DE ASÍS CUBAS y GONZÁLEZ, "Historia clínica y derechos fundamentales…", 2006.
[3331] HERNANDO, SEOANE, DE ASÍS, "La reserva...", cit., 2006, lo han entendido de la misma forma.
[3332] DÍAZ MÉNDEZ, "Historia clínica…", cit. 2004, p. 317; SEOANE, HERNANDO ROBLES, DE ASÍS CUBAS y GONZÁLEZ, "Historia clínica y derechos fundamentales…", cit., 2006: Entienden que la regulación del acceso no deberá hacerse en base a esa distinción, sino en base a criterios, básicamente, médicos. La limitación de acceso a las anotaciones subjetivas no tiene justificación.
[3333] Resolución AEPD nº R/00024/2005, procedimiento TD/00297/2004, 28 enero 2005, FJ 6.
[3334] Hay que recordar que el artículo 4.3 de la LOPD dispone que "*los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado*".

la autodeterminación informativa se ve gravemente afectado, por ejemplo, cuando datos que debieran ser cancelados porque ya no sirven para cumplir el objetivo que motivó la recogida se mantienen en los ficheros[3335]. Ya se ha visto que este conflicto se ha puesto de manifiesto en los conocidos supuestos en que diferentes personas han tratado de cancelar de los ficheros bautismales información que les vinculaba con una determinada religión. Mantener en dichos ficheros la información relativa a la vinculación de una persona a dicha religión de la que en la actualidad no participa, necesariamente afecta al derecho a la autodeterminación informativa de dichos sujetos[3336]. El TEDH ha subrayado que mantener datos que no sirven para alcanzar la finalidad que justificó la recogida de los datos afectaría negativamente a la capacidad de control que cada uno guarda sobre la información que le corresponden[3337]. Segundo, resulta obvio que la salud de las personas puede llegar a ponerse en peligro si los profesionales sanitarios emplean datos de calidad no contrastada, por ejemplo, erróneos o no rectificados, pues esta circunstancia llevaría a tomar decisiones en base a información equivocada. Ya se dijo que para que la asistencia sanitaria sea adecuada es necesario manejar una información de calidad, que refleje con la mayor precisión posible el estado de salud de las personas que van a ser atendidas.

En este marco los derechos de rectificación y cancelación constituyen herramientas indispensables para mantener la calidad de la información[3338]. Estos derechos se recogen en la LOPD desde dos perspectivas diferentes[3339]. Primero, y siguiendo lo que marcaban la Directiva europea[3340] y el Convenio del Consejo de Europa de 1981[3341], como obligaciones impuestas al responsable del fichero, dirigidas a asegurar la calidad de los datos. Con respecto a la rectificación la Ley señala que si la información recogida con un fin resulta inexacta o incompleta, será cancelada y sustituida de oficio[3342]. Por su parte, en lo que concierne a la cancelación, señala la Ley que los datos que dejen de ser necesarios o pertinentes para lograr la finalidad pretendida por el responsable del fichero han de ser cancelados[3343]. Esta perspectiva tiene su

[3335] SAN 14 septiembre 2001, FJ 3. PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 301.
[3336] GONZÁLEZ MORENO, "La Ley Orgánica de Protección…", cit., 2010, p. 608 y siguientes, en las que se analiza esta cuestión.
[3337] STEDH 4 de diciembre de 2008, S y Marper v. Reino Unido, FFJJ 68-126.
[3338] SAN 7 junio 2002, se refiere a la importancia de respetar los principios de calidad en un ámbito tan importante como los ficheros de solvencia patrimonial, donde los errores pueden hacer que una persona sea considerada morosa sin serlo.
[3339] CARDONA RUBERT, *Informática y Contrato…,* cit., 1999, pp. 114-115.
[3340] Artículo 6.1. Directiva: "*Los estados miembros dispondrán que los datos personales sean: (...) d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados*".
[3341] Artículo 5 Convenio 108/1981 del Consejo de Europa: "*Los datos de carácter personal que sean objeto de un tratamiento automatizado: d) serán exactos y si fuera necesario puestos al día*".
[3342] Artículo 4.4 LOPD: "*Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16*".
[3343] Artículo 4.5 LOPD: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos". Informe jurídico AEPD 127/2006: los principios de calidad obligan al responsable a cancelar los datos una vez cumplida la finalidad para la que fueron recogidos.

reflejo también en el reglamento que desarrolla la Ley, que viene a reproducir, en gran medida, lo dispuesto en la LOPD[3344]. Evidentemente, estas obligaciones no pueden constituir exigencias que supongan cargas desproporcionadas para los responsables de los ficheros[3345]. Por ejemplo, no puede llevar a requerir la obligación del responsable de realizar de oficio constantes investigaciones para asegurarse de que la información que posee es veraz. Fundamentalmente se impone la obligación de no alterar la información que poseen, de no perderla o de conservarla cuando se ha cumplido ya el fin que justificó su recogida.

Desde una segunda perspectiva la cancelación y la rectificación se reconocen como derechos a ejercer por el titular de los datos. En este sentido, la LOPD concreta lo que ya fijaban la Directiva europea[3346] y el Convenio citado[3347]. Señala la Ley que el responsable tendrá la obligación de hacer efectivos los derechos de rectificación y cancelación que ejerza el titular de los datos en un plazo máximo de diez días. Dispone el legislador estatal que la rectificación y cancelación de los datos se darán cuando el tratamiento de los mismos no se ajuste a los parámetros marcados por la Ley y sobre todo cuando dichos datos sean inexactos o incompletos con respecto a la realidad. Por otro lado, se señala que la cancelación conllevará el bloqueo de los datos, que se conservarán a disposición de las Administraciones públicas y la Administración

[3344] Artículo 8.5 RDLOPD: "*Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente de, afectado, se considerarán exactos los facilitados por éste.*
Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.
Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.
En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.
Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.
Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento".
Artículo 8.6 RDLOPD: "*Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*
No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.
Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento".

[3345] GUERRERO PICÓ, *El impacto de Internet...*, cit., 2006, p. 245: El artículo 6 de la Directiva exige que esa actuación de oficio sea la razonable, sin que se pueda exigir al responsable una actuación excesiva.

[3346] Artículo 12 Directiva 95/46/CE: "*Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento:*
b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos.
c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado".

[3347] Artículo 8 Convenio: "*Cualquier persona deberá poder: c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio*".

de justicia, a efectos de aclarar posibles responsabilidades derivadas del tratamiento de datos, hasta que las acciones para exigir dichas responsabilidades prescriban. Transcurrido ese plazo los datos serán suprimidos. En caso de que estos datos hubieran sido previamente cedidos a terceros, el responsable del tratamiento deberá comunicar la cancelación o rectificación a dichos sujetos para que hagan lo propio. Los datos de carácter personal deberán conservarse durante los plazos previstos en las disposiciones pertinentes o en los contratos realizados entre el responsable del tratamiento y el titular de los datos[3348]. Esta regulación encuentra desarrollo en el reglamento que concreta los preceptos de la Ley[3349].

Estas dos vertientes de la cancelación y la rectificación han tenido reflejo también en el apartado de la LOPD dedicado a la regulación de las sanciones. Se sanciona como infracción leve[3350], o muy grave en caso de que el hecho se produzca sistemáticamente[3351], el no atender por motivos formales la solicitud del titular de los datos de ejercicio de los derechos de rectificación o cancelación. Por otro lado, se sanciona como infracción grave el mantener datos de carácter personal inexactos o no efectuar la cancelación o rectificación de dichos datos, cuando estas actuaciones afecten a los derechos de las personas que la LOPD ampara[3352]. En el primer precepto se hace referencia a la rectificación y la cancelación como derechos del titular de los datos. En el segundo, estos conceptos aparecen como obligaciones del responsable. La relación entre ambas vertientes es evidente y podría plantear, a la hora de sancionar estas actuaciones, ciertos problemas interpretativos. Concretamente, podría generarse en este caso un problema de aplicación del principio *non bis in idem* en la medida en que podría parecer que en ambos preceptos se sanciona a la misma persona, por el mismo hecho y con el mismo fundamento.

Como ha señalado la jurisprudencia, ambos supuestos conllevan infracciones diferentes, que si bien están relacionadas, responden a circunstancias distintas[3353]. En el primer caso se

[3348] Artículo 16 LOPD: "*Derecho de rectificación y cancelación:*
1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado".
[3349] Artículo 31 y siguientes RDLOPD.
[3350] Artículo 44.2.a) LOPD.
[3351] Artículo 44.4.h) LOPD.
[3352] Artículo 44.3.f) LOPD.
[3353] STS 28 de octubre del 2000, FFJJ 3, 4 y 5; SAN 19 de noviembre de 2003, FJ 5: Señala el tribunal que no hay *non bis in idem*. En este caso una persona aparecía en un fichero como persona que incumplía sus deberes patrimoniales. Mantener ese dato afecta a la fama, imagen y honor, pues muestra una realidad que no se corresponde con la realidad. Y por otro lado, el incumplimiento del derecho de cancelación afecta directamente al derecho a la autodeterminación informativa. No hay vulneración del *non bis in idem*.

sanciona la vulneración del derecho a la autodeterminación por no haber atendido la reclamación de rectificación o cancelación del titular de unos datos. En el segundo, lo que se sanciona es, no tanto el mero hecho de no haber atendido la solicitud del titular de los datos, sino la circunstancia de haber mantenido datos inexactos, no veraces o no actuales, afectando a derechos como al honor, la intimidad o la imagen de la persona interesada[3354]. Piénsese el daño que puede hacer que un responsable de fichero muestre a una persona ante la sociedad como morosa cuando esa información no responde a la verdad. En conclusión, si bien es cierto que ambos preceptos guardan cierta similitud de contenido, se refieren a acciones que afectan a diferentes bienes jurídicos y, por lo tanto, pueden ser sancionadas de manera separada.

III.1.2. Definición de los conceptos de rectificación y cancelación. Especial referencia al bloqueo como efecto de la cancelación.

Corresponde ahora definir lo que hay que entender por rectificación y cancelación. A) El derecho de rectificación no plantea excesivos problemas de interpretación. Se refiere a la necesidad de que los datos se ajusten a la realidad actual[3355]. Se exige la rectificación cuando hay datos inexactos o incompletos[3356]. Estos datos deberán ser rectificados de manera que la información responda a la verdad del momento.

La importancia de que la información sea veraz y, por lo tanto, de que el derecho de rectificación pueda ejercerse de manera eficiente se ha puesto de manifiesto en otro ámbito del derecho como es el que regula la libertad de información. En este caso, la relevancia de este derecho de rectificación reside en su efecto o resultado, que no es otro que el de "reducir una cosa a la exactitud que debe tener"[3357]. Como derecho subjetivo, la rectificación constituye en este ámbito un instrumento del que dispone la persona para evitar el perjuicio que le puede causar una información errónea, por ejemplo, en su honor[3358]. Sin embargo, más allá de su consideración como derecho subjetivo, la rectificación, en la medida en que se dirige a asegurar la veracidad de la información, configura una garantía en el ejercicio de la libertad de información por los medios de comunicación, como mecanismo necesario para crear una opinión pública libre[3359]. Si la información es errónea difícilmente puede crearse un flujo de información adecuado que asegure que la sociedad tendrá los instrumentos necesarios para poder configurarse una visión propia de la realidad. En el ámbito de la protección de datos el derecho de rectificación tiene el mismo fin inmediato, que no es otro que el de buscar la veracidad de la información. Los datos se manipulan para conseguir un fin. Ese fin no se consigue si los datos que se manipulan

[3354] STSJ de Madrid 10 de marzo de 2010, FJ 2, en la que se sanciona al Ayuntamiento de Madrid por no tener datos exactos de un particular.
[3355] FREIXAS GUTIÉRREZ, *La Protección...*, cit., 2001, p. 195: "En este supuesto los datos se ajustan al contenido de la ley en todos sus aspectos excepto en el principio de veracidad, motivo por el cual la ley obliga a rectificar los inexactos o a completar los datos que así lo requieran".
[3356] Artículo 31.1 RDLOPD: "*El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos*".
[3357] CARRILLO, "Derecho a la Información…", cit., 1988, p. 191; ESTIVAL ALONSO, "El Derecho de Rectificación…", cit., 2007. LO 2/1984, 26 de marzo, reguladora del Derecho de Rectificación, artículo 1: "*Toda persona, natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio*".
[3358] STC 22 de diciembre de 1986, FJ 4.
[3359] STC 12 de marzo de 2007, FJ 8.

son erróneos o no se corresponden con la realidad actual. La rectificación constituye, pues, un instrumento imprescindible para que los datos reflejen en todo momento dicha realidad actual.

B) La regulación de la cancelación genera mayor confusión[3360], ya que la LOPD emplea indistintamente los conceptos de supresión y bloqueo como efectos de la cancelación[3361], sin que se sepa exactamente en qué momento la cancelación puede implicar una u otra operación[3362]. Señala también que los datos deberán conservarse durante un plazo determinado de tiempo cuando las normas así lo dispongan o cuando la existencia de una relación contractual obligue a ello debido a que el desarrollo del contrato depende de la manipulación de los datos[3363]. El RDLOPD la define como el procedimiento por el que el responsable del tratamiento cesa en el uso de los datos. Señala que la cancelación implica el bloqueo de los datos, que no es otra cosa que la identificación y reserva de los datos a efectos de impedir que sean manipulados, excepto para ponerlos a disposición de las Administraciones públicas, Jueces y Tribunales, para que se aclaren posibles responsabilidades derivadas del tratamiento de la información. Una vez transcurrido el plazo para llevar a cabo las acciones pertinentes para pedir responsabilidades la cancelación exigirá la supresión de los datos[3364]. La Directiva europea sobre protección de datos también hace referencia a los conceptos de supresión y bloqueo sin determinar cuándo cabe una u otra aplicación[3365]. No hace lo mismo el Convenio del Consejo de Europa de 1981, que en todo caso cita el borrado de los datos sin hacer mención alguna al bloqueo[3366].

De la normativa expuesta se deduce que la cancelación puede acarrear un doble efecto, dependiendo del momento que se trate o de la situación: la supresión o el bloqueo. No hay duda de que en todo caso la cancelación, tanto cuando conlleva la supresión como cuando implica el bloqueo, lleva a que no se puedan manipular los datos. Supone la imposibilidad de que la información pueda ser utilizada o tratada. Si posteriormente a la cancelación los datos son manipulados se estará vulnerando el ordenamiento al tratarlos sin el consentimiento del titular[3367]. Sin embargo, más allá de este efecto, la normativa prevé que esta operación puede conllevar el borrado o supresión de los datos, o su bloqueo. Apelando al sentido común, lo más corriente sería partir de un concepto que entienda que la cancelación se refiere a la supresión o eliminación[3368]. En un principio la cancelación parece sugerir que se requiere del borrado de la

[3360] SERRANO PÉREZ, "Los derechos de rectificación…", cit., 2010, p. 1.224.
[3361] Artículo 16.3 LOPD.
[3362] OROZCO PARDO, "La Protección...", cit., 2002, p. 219: "subsiste el problema de delimitar el alcance del concepto de cancelación, pues no se sabe bien si ello implica el borrado o desaparición definitiva de los datos, o sólo su almacenamiento en unas condiciones especiales que imposibiliten su acceso o comunicación".
[3363] Artículo 16.5 LOPD.
[3364] Artículo 5.1.b) RDLOPD: "*Cancelación: procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos*". FERNÁNDEZ LÓPEZ, "Algunas reflexiones…", cit., 2007, pp. 61-62, apunta la confusión que genera el RDLOPD cuando regula la figura de la cancelación.
[3365] Artículo 12.b) Directiva 95/46/CE.
[3366] Artículo 8.c) Convenio 1981 del Consejo de Europa.
[3367] Resolución AEPD R/01370/2009, 1 de junio de 2009, procedimiento PS/00032/200).
[3368] ARROYO YANES, "La Cancelación...", cit., 1994, pp. 182-185, se hace eco de este hecho; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, pp. 134-135.

información. Sin embargo, el bloqueo no conllevaría este efecto[3369], sino que supondría la conservación de los datos en circunstancias especiales[3370]. Según algún informe jurídico de la AEPD, con el bloqueo se suspende el borrado de los datos durante un plazo de tiempo[3371]. En este período el uso de los datos es muy limitado: no se pueden manipular los datos bloqueados, simplemente se conservan con un fin muy concreto, que según las normas consistiría en aclarar posibles responsabilidades que pudieran derivar de la relación entre el responsable o encargado y el titular. En algún caso se ha dicho que incluso el propio titular de los datos carece de derecho a acceder a los datos durante esta fase de bloqueo[3372]. En estos supuestos el borrado se produciría una vez hubiera transcurrido el plazo para poder exigir las citadas responsabilidades.

El principal problema que plantea esta regulación es concretar los plazos durante los que se pueden bloquear los datos. A la hora de fijar estos plazos puede generarse cierta confusión. Cuando la LOPD se refiere a las responsabilidades cuya aclaración justificaría el bloqueo hace referencia a las "responsabilidades nacidas del tratamiento". Parece, por lo tanto, que sólo habría de considerarse el plazo para exigir responsabilidades que pudieran derivar del tratamiento de datos para determinar el plazo durante el que deben permanecer los datos bloqueados. Del RDLOPD se desprende que la responsabilidad puede derivar no sólo del tratamiento sino de otro tipo de relación de la que pudiera generarse otra responsabilidad como la penal, civil, o administrativa, pues su texto se refiere a las responsabilidades que pudieran nacer de la relación existente entre el titular de los datos y el responsable[3373]. Parece evidente que será difícil determinar la responsabilidad de una persona por haber manipulado unos datos de manera contraria a Derecho si dichos datos son suprimidos y se borra la existencia de los mismos[3374]. La normativa de protección de datos debía haber determinado estos plazos. A falta de esta previsión deberá acudirse a la normativa común para fijarlos[3375]. Cuando se trata de exigir responsabilidades por incumplimiento de la LOPD, el plazo será de tres, dos o un año, dependiendo de si la infracción es muy grave, grave o leve, respectivamente, a contar desde el

[3369] Resolución AEPD, R/01259/2009, procedimiento PS/00040/2009: Se refiere al bloqueo como acción que "implica que los datos personales se encierran, aíslan o incomunican de tal manera que resulta imposible su ulterior tratamiento o utilización".

[3370] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 317.

[3371] Informe jurídico AEPD, "Bloqueo de Datos de Carácter Personal", nº 0000/2001, 2001, en http://www.agpd.es "*(...)* existirán determinados supuestos en que la cancelación o bien no podrá tener lugar, dada la obligación impuesta por la Ley, o bien deberá suponer una fase previa de bloqueo de los datos que, produciendo unos efectos similares al borrado físico de los mismos, salvo en determinadas circunstancias, no implicará automáticamente ese borrado"

[3372] COUDERT, "Ejercicio de Derechos…", cit., 2007 p. 412: el derecho de acceso no procede cuando los datos están bloqueados; ALMUZARA ALMAIDA, "Relaciones precontractuales…", cit., 2007, p. 212: el bloqueo hace que los datos sometidos a ese régimen dejen de estar disponibles para nadie salvo para la Administración y Jueces y Tribunales. Ni siquiera el titular de los datos puede acceder.

[3373] Artículo 8.6 RDLOPD. PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 307.

[3374] Informe jurídico AEPD 182/2003: si no fuera posible el bloqueo la AEPD no podría aclarar las responsabilidades que derivaran de los tratamientos. Por ello la cancelación no conlleva siempre el borrado automático de los datos. DAVARA RODRÍGUEZ, *Guía Práctica de Protección…,* cit., 2006, p. 92: "cancelación no es lo mismo que borrado; la cancelación no puede exigir el borrado total y absoluto de los datos, aunque sea necesario el bloqueo con todas las características de seguridad que le deban acompañar; de otra manera, nos encontraríamos ante la extraña situación de que el borrado total de los dato no permitiría atender otras obligaciones, porno existir ya rastro alguno sobre los datos, como pueden ser los requerimientos realizados por los Jueces y Tribunales, o por la propia Administración".

[3375] MARTÍNEZ MARTÍNEZ, *Tecnologías de la información…,* cit., 2001, p. 240: sería bueno que reglamentariamente se estableciera el plazo durante el que se puede bloquear la información antes de su supresión.

día en que la infracción se hubiera cometido[3376]. Cuando se trata de exigir responsabilidad civil por las obligaciones derivadas de la generación de un daño por culpa o negligencia, existirá el plazo de un año desde que el agraviado conoció la existencia del daño[3377]. En el ámbito penal los delitos prescriben y la responsabilidad criminal se extingue, dependiendo de su naturaleza[3378]. Cuando se trata de exigir la responsabilidad a la Administración debido a un daño creado por la actuación del personal al servicio de ésta, el derecho a reclamar dicha responsabilidad prescribirá al año de haberse producido el hecho o el acto que motiva la indemnización, o, en caso de que se trate de daños físicos o psíquicos, cuando éstos se hayan curado o se haya podido determinar el alcance de las secuelas.[3379]. Una vez transcurrido el plazo para exigir dichas responsabilidades se deberán suprimir los datos, pues el motivo que justifica la conservación ha desaparecido.

No hay que confundir este bloqueo con la obligación que imponen determinadas leyes, por ejemplo en el ámbito sanitario, o la existencia de una relación contractual de conservar datos de carácter personal. La LOPD reconoce la posibilidad de que leyes o exigencias de origen contractual impongan la obligación de conservar unos datos. Parece que en algún informe de la AEPD se confunde esta obligación con el bloqueo de los datos[3380]. Hay que distinguir ambos supuestos. El bloqueo lleva a que los datos no puedan ser manipulados y a que se paralice su tratamiento, como si se hubieran borrado, así como a su conservación a los solos efectos de aclarar posibles responsabilidades de las personas implicadas en el tratamiento de los datos. En cambio, la obligación de conservar impuesta por una Ley o por la existencia de una relación contractual cuyo desarrollo requiere de la manipulación de los datos, no acarrea el efecto del bloqueo. La obligación de conservar se fija con el objetivo de que los datos puedan ser manipulados con determinados fines, más allá de la exigencia de responsabilidades. En el caso del ámbito sanitario, como se verá, se conservarán los datos con fines como la asistencia sanitaria o la investigación. En este supuesto se entiende que existe un bien jurídico de relevancia que hace que la cancelación no pueda llevarse a cabo. Cuando existe una relación contractual en vigor entre el titular de los datos y el responsable, evidentemente no se podrán cancelar unos datos que están siendo empleados para el desarrollo de dicha relación[3381]. El bloqueo es una forma de cancelación. La obligación de conservación, por el contrario, es una excepción al derecho a cancelar.

El bloqueo no es una alternativa a la cancelación sino que parece ser un efecto de la misma, que en algunos casos ha de darse en vez de la supresión de los datos[3382]. La principal cuestión a

[3376] Artículo 47 LOPD.
[3377] Artículo 1968 CC, en relación con el 1902 CC.
[3378] Artículo 131 CP.
[3379] Artículo 142.5 LPAC.
[3380] Informe jurídico AEPD, "Bloqueo de Datos de Carácter Personal", nº 0000/2001, 2001, en http://www.agpd.es
[3381] Resolución AEPD R/01322/2008, 7 de octubre de 2008, procedimiento TD/00541/2008: Evidentemente, no pueden cancelarse unos datos si persiste una relación entre el responsable y el titular de los datos que requiere de la manipulación de dicha información. Cosa que ocurre si se quieren anular los datos de una entidad bancaria pero a su vez mantener una cuenta corriente en dicha entidad.
[3382] Resolución de la AEPD R/01473/2009, 24 de junio de 2009, procedimiento TD/00024/2009: en la que un responsable contesta a un interesado que no puede proceder a la cancelación debido a que la Ley le obliga a conservar los datos durante los períodos de tiempo legalmente establecidos. La AEPD señala que el bloqueo es una consecuencia de la cancelación, no una alternativa.

plantear es cuándo la cancelación lleva al bloqueo y cuándo a la supresión de la información. De lo dispuesto por las normas no es fácil responder a esta cuestión. De la redacción de la Ley parece desprenderse que la cancelación dará lugar, en todo caso, al bloqueo, conservándose los datos para la aclaración de posibles responsabilidades. Una vez transcurrido el plazo para exigir responsabilidades se pasaría a la supresión de los datos. Sin embargo, el reglamento que desarrolla la Ley afirma que la cancelación producirá la supresión, salvo en los casos en que sea necesario el bloqueo. La norma general parece ser aquí el borrado y no el bloqueo[3383]. Cercana a esta regulación parecía situarse la normativa anterior a la entrada en vigor del nuevo reglamento[3384]. Tampoco la jurisprudencia ni las resoluciones de la AEPD llegan a aclarar este punto. Esta última simplemente ha señalado que no siempre que se ejerce la cancelación ha de procederse al bloqueo, sino cuando una Ley lo señale o de la relación entre el titular de los datos y el responsable del fichero deriven responsabilidades[3385].

Para deducir cuándo la cancelación produce uno u otro efecto deberá aclararse, primero, cuándo procede la cancelación. De la Ley se desprende que la cancelación puede darse cuando los datos son contrarios a lo dispuesto por la ley o no son necesarios para cumplir la finalidad que motivó su recogida[3386]. El reglamento que desarrolla la Ley suma a estas causas el supuesto en que el titular de los datos revoca el consentimiento necesario que emitió para su tratamiento[3387]. Parece lógica esta previsión, en la medida en que si el titular desautoriza el tratamiento inicialmente consentido, la posterior manipulación será necesariamente contraria a Derecho. Segundo, habrá que tener en consideración que la finalidad del bloqueo no es otra que la de conservar los datos para que puedan ser empleados por la Administración o Jueces y Tribunales en la depuración de posibles responsabilidades que pudieran derivar de la relación entre el responsable o encargado del fichero y el titular de los datos.

Teniendo en cuenta cuándo se dará la cancelación y cuál es la finalidad del bloqueo puede aclararse cuándo procede la supresión y cuándo el bloqueo. El bloqueo procederá cuando la supresión sea físicamente imposible. Más allá de este caso, dependerá de las posibilidades reales de que de la relación entre el titular de los datos y el responsable o encargado nazcan responsabilidades, es decir, de la potencialidad de la relación para que de ella deriven responsabilidades. Por ejemplo, la supresión podrá darse cuando la relación entre el titular de los

[3383] Artículo 31.2 RDLOPD: "*El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento*".

[3384] Norma tercera Instrucción 1/1998 AEPD: "*8-La cancelación exige el borrado físico de los datos, sin que sea suficiente a estos efectos una marca lógica o el mantenimiento de otro fichero alternativo en el que se registren las bajas producidas. 9-En los casos que, siendo procedente la cancelación de los datos, no sea posible su extinción física, tanto por razones técnicas como por causa del procedimiento o soporte utilizado, el responsable del fichero procederá al bloqueo de los datos, con el fin de impedir su ulterior proceso o utilización*".

[3385] Informe jurídico AEPD 339/2008: el bloqueo no parece automático para todos los casos en que se ejerza la cancelación sino que vendrá en dos casos: cuando lo disponga así una norma con rango de Ley o de la relación en que se produzca la cancelación pudieran derivar responsabilidades, sobre todo, para el responsable del fichero. En este último caso habrá que estar a los plazos de prescripción de las acciones que pudieran derivarse de la relación que vincula a los sujetos implicados. FATÁS y GARCÍA SANZ, "Título Primero…", cit., 2008, p. 121.

[3386] Artículo 4.5 LOPD y 16.2 LOPD.

[3387] Artículo 31.2 RDLOPD: "*(...) En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento*".

datos y el responsable finaliza de mutuo acuerdo. En estos casos no parece que tenga sentido bloquear los datos, debiendo procederse a la supresión automática. Es el caso también en que el titular de los datos ejerce su derecho a la oposición y el responsable acepta dicho ejercicio. En este supuesto no parece que tenga sentido el previo bloqueo, en la medida en que hay una posición sobre la que no surge problema alguno.

III.1.3. Sobre el ejercicio de los derechos de rectificación y cancelación, y sus límites.

El ejercicio de la cancelación o rectificación ha de seguir las reglas marcadas por el RDLOPD. La solicitud de rectificación, más allá de los requisitos comunes señalados para la solicitud del ejercicio de cualquiera de los derechos que ahora se analizan, debe contener la referencia de los datos que se quieren corregir, la corrección de los mismos, es decir, la referencia a los veraces, y la documentación que justifica lo solicitado. Cuando lo solicitado es la cancelación deberá determinarse qué datos se quieren cancelar y, en su caso, la documentación que justifica dicho ejercicio. El responsable del fichero deberá resolver la solicitud en el plazo de diez días a contar desde la recepción de la solicitud y notificar la solución al titular de los datos. En caso de que no lo haga, el titular de los datos podrá interponer la reclamación de tutela de los derechos. Si el responsable no cuenta con datos de quien ejerce dichos derechos deberá ponerlo en conocimiento del interesado en el mismo plazo de diez días. Al igual que ocurriera con el ejercicio del derecho de acceso, se entiende que no se cumple por parte del responsable del fichero su obligación de responder a la solicitud del titular de los datos hasta que el primero no contesta en plazo al segundo[3388]. En caso de que el responsable del fichero hubiera transmitido los datos a un tercero, deberá comunicar en el mismo plazo la rectificación o cancelación a este cesionario, para que este último, en diez días a contar desde la recepción de la comunicación, rectifique o cancele los datos pertinentes. Esta rectificación o cancelación del cesionario no necesita ser comunicada al interesado[3389].

Hay que subrayar la ampliación del plazo para resolver de cinco días, que establecía la LORTAD, a diez días, que establecen la LOPD y el reglamento que la desarrolla. Como ha señalado la doctrina, parece correcta la ampliación, pues el intervalo de cinco días resultaba demasiado corto para hacer efectivos dichos derechos[3390]. El cómputo de estos plazos se realizará de acuerdo a los criterios fijados en el apartado dedicado al acceso.

El reglamento impone al afectado que ejerce la cancelación o rectificación la obligación de indicar el dato que es erróneo y señalar la corrección oportuna, facilitando así la labor del responsable del fichero[3391]. Se trata de una disposición a valorar positivamente, pues, como se ha visto al analizar los principios relativos a la calidad, la obligación que la LOPD impone al

[3388] SAN 1 de junio de 2005, FJ 4, en que se entiende que no se ha hecho efectiva la cancelación pues, a pesar de redactar la contestación el responsable, no se notificó en plazo de 10 días al titular de los datos. Resolución AEPD, R/00220/2008, 3 de marzo de 2008, procedimiento TD/00754/2007: la AEPD concluye que no se ha completado el derecho de cancelación pues, a pesar de haber eliminado la información del fichero no se ha notificado dicho hecho al titular de los datos.
[3389] Artículo 32 RDLOPD.
[3390] DEL PESO NAVARRO, *Ley de Protección*..., cit., 2000, p. 54.
[3391] Resolución APDCM, 19 de mayo de 2009, "El derecho de cancelación debe referirse a datos personales concretos".

responsable del fichero de que, de oficio, cambie los datos erróneos por los correctos y actualizados[3392], podía llevar a entender que recae en la figura del responsable del fichero la obligación de recabar por su cuenta la información necesaria para llevar a cabo la rectificación. Esta exigencia resultaría completamente desproporcionada. Requerir al titular de los datos que facilite la labor del responsable del fichero resulta una medida a valorar positivamente.

Las excepciones a la posibilidad de ejercer la cancelación o la rectificación son las previstas para todos los derechos de las personas, y que ya se han analizado más arriba. Más allá de estos supuestos el RDLOPD especifica para los derechos de cancelación y rectificación una serie de casos en que el responsable puede denegar al titular de los datos el ejercicio de los mismos.

En primer lugar, siguiendo lo que prevé la LOPD, el reglamento reconoce el caso ya citado en que bien por Ley o por la existencia de relaciones contractuales, se obliga al responsable a conservar los datos durante un plazo determinado de tiempo[3393]. En estos supuestos la conservación deberá estar justificada para el cumplimiento de determinados fines. Sólo se conservarán los datos que sean necesarios para el cumplimiento de dichos fines[3394].

En segundo lugar, el reglamento reconoce también la posibilidad de denegar los derechos de rectificación y cancelación cuando así lo prevea una ley o norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso[3395]. Evidentemente, en el último supuesto, si se deniega el derecho de acceso del titular, se estará exceptuando también la cancelación o rectificación. Si no se revela al interesado la información que se está manipulando difícilmente podrá ejercer la rectificación o cancelación.

En caso de denegar el ejercicio de estos derechos, el responsable del fichero deberá informar al titular de los datos sobre la posibilidad de acudir a la agencia de protección de datos correspondiente para recabar la oportuna tutela[3396].

III.2. La rectificación y cancelación en el ámbito sanitario.

Se han subrayado los principales problemas de interpretación que plantea la regulación de los derechos de rectificación y cancelación en la normativa de protección de datos. Es necesario analizar ahora las dificultades prácticas que en el ámbito sanitario genera el ejercicio de estas

[3392] Artículo 4.4 LOPD.
[3393] Artículo 33.1 RDLOPD; Artículo 16.5 LOPD.
[3394] Plan de Inspección de Oficio al INAP, Diciembre de 2004, pone de manifiesto como el INAP conserva datos de antiguos alumnos o profesores que han impartido algún curso hace años. Se recomienda que delimite la finalidad a la que se destina dicha información y, en caso de que no cumpla finalidad alguna en la actualidad, se bloqueen dichos datos. Asimismo se recomienda que determine un procedimiento concreto para que los interesados puedan ejercer sus derechos. Plan de Inspección de Oficio a Cadenas Hoteleras, junio 2004: en numerosas ocasiones en los hoteles se mantiene información sobre antiguos clientes que en determinadas fechas se hospedó en dicho establecimiento, sin que esté clara la finalidad perseguida por esta actuación. Debe definirse la finalidad que se persigue con dichos actos: facturación…
[3395] Artículo 33.2 RDLOPD.
[3396] Artículo 33.3 RDLOPD.

facultades, pues las particularidades de este sector harán que la posibilidad de ejercerlas se vea limitada en múltiples supuestos.

III.2.1. Cuestiones generales y el ejercicio del derecho de rectificación.

En el ámbito sanitario los derechos de cancelación y rectificación presentan sus particularidades. En este entorno el tratamiento de los datos no es más que un medio para la consecución de un fin concreto, como es el de la defensa del derecho a la salud que a todos asiste. No es difícil entender que la actualización de la información, y la supresión de los datos que no sirven para cumplir los objetivos, supondrá un activo importante para obtener los mejores resultados en la asistencia sanitaria y demás objetivos que componen el fin genérico de la protección de la salud.

La normativa sanitaria exige expresamente que la historia clínica responda en todo momento a criterios de veracidad y actualidad[3397]. Así, rectificar los datos erróneos o incompletos y cancelar, o bloquear en su caso, los que ya no sirven para llevar a cabo la finalidad perseguida supone una actividad de importancia para conseguir este fin. Más allá de esta previsión, las normas que regulan la materia sanitaria no realizan aclaraciones concretas sobre la posibilidad de ejercer, por parte del paciente, los derechos de cancelación o rectificación sobre la documentación médica, y simplemente determinan la obligación de conservar dicha documentación durante diferentes plazos de tiempo dependiendo de la finalidad. En protocolos de actuación internos como los que afectan al Sistema Vasco de Salud el reconocimiento de la posibilidad de ejercer los derechos de la persona se ve reflejado con la asunción de los contenidos de la normativa de protección de datos[3398]. Por su parte, la normativa de protección de datos tampoco hace referencia a esta cuestión. Desde el ámbito internacional, la Recomendación del Consejo de Europa sobre la protección de los datos médicos no realiza una regulación amplia y suficiente de dichos derechos, y únicamente reconoce la posibilidad de ejercer el derecho de rectificación en este ámbito[3399] y la obligación de conservar los datos sanitarios durante un plazo de tiempo determinado[3400]. Las citas a esta cuestión en la jurisprudencia tampoco son muy amplias y, al igual que ocurre con la actuación de la AEPD, la mayoría de los análisis al respecto se centran en la posibilidad o no de cancelar los datos sanitarios. El estudio de los derechos de rectificación y cancelación aplicados al sector sanitario deberá partir, por lo tanto, de la consideración de lo que se ha explicado arriba sobre el contenido y ejercicio de estos derechos.

El derecho a la rectificación cuenta con plena vigencia en el ámbito sanitario. El responsable del fichero tiene la obligación de corregir los datos que sabe que no son correctos y el titular de los datos tiene, igualmente, el derecho a llevar a cabo las correcciones que estime oportunas. El ejercicio de este derecho no plantea mayores problemas que los expuestos en el apartado

[3397] Artículo 15.1 LBAP: "*La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente (...)*".
[3398] Instrucción 6/2003, 2 de septiembre de 2003, Director General de Osakidetza, sobre Funciones y obligaciones del personal de Osakidetza/Servicio vasco de salud, con relación a la protección de datos de carácter personal.
[3399] Artículo 8.3 R (97) 5.
[3400] Artículo 10 R (97) 5.

anterior cuando se trata de datos, que obran en su mayor parte en ficheros administrativos y que se refieren a datos puramente objetivos que mayormente no conciernen directamente a la salud. En el ámbito sanitario el problema con respecto a la facultad de rectificar se produce principalmente por dos circunstancias.

En primer lugar, se puede plantear la situación en que un paciente o usuario solicite rectificar unos datos que en el pasado fueron ciertos pero en el presente no lo son, debido a que la situación de dicho sujeto ha variado. Piénsese en el caso de una persona que sufrió determinada enfermedad ya superada o en el supuesto en que un sujeto era drogodependiente y ahora no. En estos casos la solicitud del titular de los datos de rectificar y actualizar dicha información se hará efectiva o no dependiendo de una circunstancia: habrá que ver si la conservación de la información pasada puede resultar pertinente para cumplir fines concretos, como la asistencia al propio sujeto o la protección de la salud de terceros[3401].

En segundo lugar, los problemas pueden derivar por el hecho de que cuando se trata de documentación sanitaria mucha información resulta de valoraciones, diagnósticos y aclaraciones subjetivas y, además, se trata de información especialmente técnica. Con respecto a esta última cuestión se entiende aquí, que teniendo en cuenta que la información sanitaria es especialmente compleja a la hora de ser interpretada, hay que tener especial cuidado en el momento de hacer efectivo este derecho. Debido a esa complejidad puede ocurrir que el propio paciente desconozca con exactitud el significado de los datos que pretende rectificar. Por ello se interpreta que la rectificación, si bien hay que considerarla como derecho del paciente de primer orden, hay que ejecutarla con asistencia, para que no pueda suponer una merma de la calidad de los datos[3402]. Esta idea viene reforzada con la previsión normativa de que corresponde a los profesionales sanitarios la elaboración y composición de las historias clínicas[3403], por lo que parece que dicho profesional ha de tener cierta participación, incluso a la hora de que el paciente o usuario lleve a cabo la rectificación.

Por último, las dificultades podrían generarse por el hecho de que a la hora de rectificar pronósticos, valoraciones o diagnósticos podrían surgir diferencias entre el paciente y el profesional sanitario. Esto podría pasar, por ejemplo, cuando el paciente acude a solicitar una segunda opinión medica que contradice la fijada en la documentación a la que previamente accede. Evidentemente, teniendo en cuenta la importancia de la información en el ámbito sanitario, no debería procederse a la rectificación hasta que se decidiera la viabilidad del ejercicio de este derecho[3404]. En última instancia, serían los tribunales los que debieran decidir al

[3401] GÓMEZ PIQUERAS, "La historia clínica…", cit., 2009, p. 147.
[3402] Memoria de la AEPD 2004, p. 82.
[3403] Artículo 15.3 LBAP: "*La cumplimentación de la historia clínica, en los aspectos relacionados con la asistencia directa al paciente, será responsabilidad de los profesionales que intervengan en ella*".
[3404] Resolución de la AEPD R/01658/2008, 28 de noviembre de 2008, procedimiento TD/00919/2008: en alguna ocasión se ha pretendido ejercer la rectificación no sobre informaciones objetivas sino sobre apreciaciones o valoraciones de carácter técnico. Evidentemente, la Agencia señaló que no era competente para determinar la veracidad de una apreciación. COUDERT, "Ejercicio de Derechos…", cit., 2007 p. 413: pueden existir discrepancias sobre la conveniencia o no de la rectificación entre el titular de los datos y el responsable. Las diferencias de criterio no las debe dirimir la AEPD, sino los tribunales. En todo caso, mientras se entienda que hay motivos para mantener los datos como están no se procederá a la rectificación.

respecto. De todas formas, los tribunales tampoco tienen un amplio margen de actuación a la hora de determinar la veracidad de las informaciones sanitarias. Se trata de datos especialmente técnicos, que podrían ser rebatidos basándose en una nueva opinión médica. Lo que sí podrían hacer los tribunales es verificar si ante la solicitud de rectificación del titular de los datos el responsable ha obrado debidamente atendiendo dicha solicitud[3405].

III.2.2. El derecho a cancelar los datos y la obligación de conservar la información en el ámbito sanitario.

III.2.2.A. La obligación de conservar los datos en el ámbito sanitario.

El ejercicio del derecho de cancelación en el ámbito sanitario presenta mayores problemas de interpretación que los expuestos para el derecho de rectificación. Evidentemente, cuando el tratamiento de unos datos es contrario a la Ley no hay ninguna duda sobre la pertinencia de la cancelación. Lo mismo ocurre cuando los datos han dejado de ser necesarios para cumplir el fin pretendido. Los problemas comienzan cuando la cancelación quiere llevarse a cabo por mostrarse el titular de los datos contrario al tratamiento que se está llevando a cabo. En este caso, la voluntad del interesado choca con los fines que se persiguen en este sector. En el ámbito sanitario, este derecho está reñido con la obligación que los centros tienen de conservar las historias clínicas con el fin, primero, de otorgar una asistencia sanitaria adecuada y, segundo, con otros fines de interés general como pueden ser la investigación o la realización de estudios epidemiológicos, el control de gastos, la realización de estadísticas, etc.

En principio se ha de considerar que el derecho de cancelación está plenamente vigente incluso en el ámbito sanitario. Sin embargo, en este sector la cancelación no resulta la mayoría de veces automática, teniendo que conservarse los datos durante un determinado plazo de tiempo para el cumplimiento de determinados fines[3406]. Con la obligación de conservar, en el ámbito sanitario el derecho de cancelación aparece limitado. Esta circunstancia ha hecho que se haya llegado a señalar por la doctrina que tal derecho no existe en este sector[3407]. También se ha

[3405] STSJ de la Rioja, 17 de octubre de 2008, FJ 2: en relación a la posibilidad de que el paciente pueda rectificar la información contenida en una historia clínica, señala que según el ordenamiento corresponde a los profesionales la composición y elaboración de la historia clínica, constituyendo una tarea de recopilación y valoración técnica, difícilmente revisable en vía jurisdiccional. Además, señala el tribunal que la LBAP no recoge el derecho de rectificación, por lo que parece que recae sobre la responsabilidad de los profesionales la elaboración de una historia veraz y completa y actualizada. Lo único que podría hacer el tribunal es verificar si ante la petición de rectificación del interesado el centro sanitario ha dado una respuesta adecuada y fundamentada. Otra cosa sería si el interesado presenta, por ejemplo, informes médicos de una segunda opinión que desmienten lo que el principal profesional sanitario ha apuntado y valorado en la historia clínica. En este caso se debería valorar la posibilidad de rectificar el contenido de la HC.

[3406] Informe jurídico AEPD, "La Cancelación de los Datos contenidos en Historias Clínicas", nº 189/2003, 2003, en http://www.agpd.es. Resolución de la AEPD R/01103/2009, 20 de abril de 2009, procedimiento TD/00342/2009. Se niega a un interesado el derecho a cancelar los datos contenidos en HC. También Resolución AEPD R/01424/2008, 10 de noviembre de 2008, procedimiento TD/00630/2008. MARTÍNEZ-CAMPELLO, "La Ley 41/2002…", cit., 2004, p. 190.

[3407] ATELA BILBAO y GARAY ISASI, "Ley 41/2002...", cit., 2004, pp. 52-54; MÉJICA, "Hacia un Estatuto...", cit., 2002: "el derecho de cancelación de la Ley 15/1999, en mi opinión no es aplicable al dato de salud, pues no puede cancelarse por el paciente; éste sólo puede exigir que se garantice su custodia, conservación y confidencialidad"; TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 50: "en el ámbito sanitario la cancelación de los datos es de enorme dificultad ya que está en contradicción con la eficacia de la gestión sanitaria y la necesidad de mantener el

sugerido que la cancelación en el ámbito sanitario sólo puede exigirse referida a los datos erróneos de la historia clínica[3408]. Es de tener en cuenta que se está haciendo referencia a la conservación, no a la figura del bloqueo reconocido en la LOPD. En la normativa sanitaria se establece la obligación de conservar los datos para cumplir con una serie de objetivos[3409]. En la medida en que los datos no han sido bloqueados, sino que se conservan con una serie de fines, los derechos del titular quedarán vigentes durante el plazo de conservación.

La LOPD dispone que los datos de carácter personal deberán conservarse durante el tiempo que establezcan las disposiciones[3410]. Esta previsión es completamente acorde con lo dispuesto en la Directiva europea[3411]: La LBAP señala que los centros están obligados a conservar los datos en condiciones que garanticen su mantenimiento y seguridad, con el fin de otorgar la debida asistencia, durante el tiempo adecuado, mínimo de cinco años a contar desde la fecha del alta de cada proceso asistencial[3412]. Otros fines como los judiciales, los estudios epidemiológicos, las investigaciones, la organización y el funcionamiento de los sistemas sanitarios también justifican en la Ley la conservación de los datos de carácter personal, si bien, en la medida de lo posible, la conservación de estos datos se hará de manera que éstos aparezcan disociados[3413]. En la normativa autonómica los plazos se concretan y en muchos casos se amplían. En el caso de la Comunidad Autónoma del País Vasco la normativa fija plazos distintos para documentos diferentes, teniendo en cuenta la finalidad e importancia de los mismos[3414]. En el de Cataluña

contenido completo de la historia clínica, que evite el error en las valoraciones o la repetición de pruebas diagnósticas".

[3408] Informe sobre adecuación de determinados aspectos de la Ley Orgánica de Protección de Datos de Carácter Personal al Proyecto Osabide, complementario a la Exposición realizada por el Consejero de Sanidad durante su comparecencia ante la Comisión de Sanidad del Parlamento Vasco el 23 de mayo de 2002, a fin de dar cuenta del proceso de Centralización de los Datos de los Pacientes recogidos en los Centros de Salud de Osakidetza, 31 mayo 2002, p. 19: "El derecho de cancelación deberá entenderse limitado sólo a los datos erróneos, sin alcanzar a la totalidad de la historia clínica".

[3409] Informe jurídico AEPD 0049/2005 e Informe jurídico AEPD 189/2003 e Informe Jurídico AEPD 151654/2007: cancelación de datos de una historia clínica. La solicitud de cancelación queda sujeta a la obligación de conservar la información clínica durante el plazo establecido por la LBAP. Ni siquiera cabe el bloqueo, por cuanto que la conservación de los datos se realiza para cumplir una serie de finalidades.

[3410] Artículo 16.5 LOPD.

[3411] Artículo 6.1.e) Directiva 95/46/CE: "*Los Estados miembros dispondrán que los datos personales sean: e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos"*.

[3412] Artículo 17.1 LBAP: "*Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial*".

[3413] Artículo 17.2 LBAP: "*La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas*". TRONCOSO REIGADA, *Protección de Datos*…, cit., 2008, pp. 46-47: en el ámbito sanitario resulta necesario conservar datos de carácter personal más allá de que se haya cumplido su finalidad inicial, para cumplir fines de investigación o epidemiológicos.

[3414] Artículos 9 Decreto 45/1998: "*Los documentos clínicos generados en los Servicios de Urgencias respecto de episodios asistenciales que cursen sin ingreso del paciente en el Hospital sólo podrán ser destruidos a partir de los dos años desde la fecha en que tales episodios tengan lugar, a excepción de las Hojas de Urgencias. Estas últimas sólo podrán ser destruidas a partir de los cinco años de la citada fecha"*.

ocurre lo mismo[3415], así como en el de Galicia[3416]. La Recomendación del Consejo de Europa también recoge la obligación de conservación[3417]. La AEPD ha subrayado la obligación de conservar los datos, que persiste incluso cuando un centro va a cesar en su actuación[3418].

Artículo 10: "*1. Podrán ser destruidos a partir de los cinco años desde la fecha del alta correspondiente al último episodio asistencial en que el paciente haya sido atendido en el Hospital los siguientes documentos contenidos en su historia clínica: a) las Hojas Clínico-Estadísticas; b) las Hojas de Autorización de acceso; c) las Hojas de Órdenes Médicas; d) las Hojas de Interconsulta; e) las Hojas de Infección Hospitalaria; f) las Hojas de Evolución y Planificación de Cuidados de Enfermería; g) las Hojas de Aplicación Terapéutica; h) las Hojas de Gráficas de Constantes; i) las Hojas de Urgencias; j) las Radiografías u otros documentos iconográficos; k) otros documentos que no aparezcan citados en el artículo siguiente.*
2. Igualmente, podrán destruirse, a partir de los cinco años, las Hojas de Anamnesia y Exploración Física y las de Evolución correspondientes a los episodios asistenciales sobre los que exista informe de alta".
Artículo 11: "*1. Se conservarán de manera definitiva los siguientes Tipos Documentales: a) las Hojas de Informes Clínicos de Altas; b) las Hojas de Alta Voluntaria; c) las Hojas de Consentimiento Informado; d) las Hojas de Informes Quirúrgicos y/o de Registro del Parto; e) las Hojas de Anestesia; f) las Hojas de Informes de Exploraciones Complementarias; g) las Hojas de Informes de Necropsia.*
2. Así mismo, deberán conservarse las Hojas de Anamnesia y Exploración Física y las de Evolución correspondientes a los episodios asistenciales sobre los que no exista informe de Alta.
3. Para garantizar la conservación indefinida de los citados Tipos Documentales y de la información registrada en los mismos, se utilizarán los soportes documentales más adecuados, sustituyéndose el papel únicamente en los casos en que se garantice la permanencia del soporte que se adopte para reemplazarlo".

[3415] Artículo único Ley 16/2010, 3 de junio, de modificación de la Ley 21/2000, de 29 de diciembre, sobre los Derechos de Información Concerniente a la Salud y la Autonomía del Paciente, y la Documentación Clínica: "*4. De la historia clínica debe conservarse, junto con los datos de identificación de cada paciente, como mínimo durante quince años desde la fecha de alta de cada proceso asistencial, la siguiente documentación:*
a) Las hojas de consentimiento informado; b) Los informes de alta; c) Los informes quirúrgicos y el registro de parto; d) Los datos relativos a la anestesia; e) Los informes de exploraciones complementarias; f) Los informes de necropsia; g) Los informes de anatomía patológica.
5. Los procesos de digitalización de la historia clínica que se lleven a cabo deben facilitar el acceso a la historia clínica desde cualquier punto del Sistema Nacional de Salud. A tal efecto, deben establecerse los mecanismos para hacer posible, mediante la tarjeta sanitaria individual, la vinculación entre las historias clínicas que cada paciente tenga en los organismos, centros y servicios del Sistema Nacional de Salud, y que permitan el acceso de los profesionales sanitarios a la información clínica y el intercambio de dicha información entre los dispositivos asistenciales de las comunidades autónomas, de conformidad con las disposiciones sobre protección de datos de carácter personal.
6. La documentación que integra la historia clínica no mencionada por el apartado 4 puede destruirse una vez hayan transcurrido cinco años desde la fecha de alta de cada proceso asistencial.
7. No obstante lo establecido por los apartados 4 y 6, debe conservarse de acuerdo con los criterios que establezca la comisión técnica en materia de documentación clínica, a la que hace referencia la disposición final primera, la documentación que sea relevante a efectos asistenciales, que debe incorporar el documento de voluntades anticipadas, y la documentación que sea relevante, especialmente, a efectos epidemiológicos, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. En el tratamiento de esta documentación debe evitarse identificar a las personas afectadas, salvo que el anonimato sea incompatible con las finalidades perseguidas o que los pacientes hayan dado su consentimiento previo, de acuerdo con la normativa vigente en materia de protección de datos de carácter personal. La documentación clínica también debe conservarse a efectos judiciales, de conformidad con la normativa vigente.
8. La decisión de conservar la historia clínica, en los términos establecidos por el apartado 7, corresponde a la dirección médica del centro sanitario, a propuesta del facultativo o facultativa, previo informe de la unidad encargada de la gestión de la historia clínica en cada centro. Esta decisión corresponde a los propios facultativos cuando desarrollen su actividad de forma individual.
9. Los responsables de custodiar la historia clínica, a quienes se refiere el apartado 1, también son responsables de destruir correctamente la documentación que previamente se haya decidido expurgar.
10. En el supuesto de cierre de centros y servicios sanitarios, o de cese definitivo de actividades profesionales sanitarias a título individual, debe garantizarse el mantenimiento del acceso legalmente reconocido a las historias clínicas que se encuentren bajo la custodia de dichos centros o profesionales, en beneficio de la asistencia médica y, especialmente, de los derechos de los pacientes en materia de documentación clínica y de protección de datos personales".

La redacción de las normas señaladas plantea la cuestión de si es posible en determinados supuestos una conservación *sine die* de los datos sanitarios. Como se ha visto, parece que hay fines que justifican que los datos puedan conservarse por tiempo indefinido, pues la normativa no establece límite alguno[3419]. La propia LBAP fija un plazo mínimo de conservación pero no establece un plazo máximo, por lo que parece que pueden conservarse los datos por tiempo indeterminado[3420]. En la normativa vasca la obligación de conservar algunos documentos de manera indefinida se prevé de manera expresa[3421]. Ante esta situación acertadamente ha señalado la doctrina la conveniencia de aprobar una norma que fije con mayor precisión los plazos durante los que se han de conservar los datos y el alcance real del derecho de cancelación[3422], pues la indeterminación del contenido de la normativa es evidente[3423].

III.2.2.B. La necesidad de reinterpretar la obligación de conservar los datos.

La posibilidad de que los datos puedan conservarse durante tiempo indefinido genera cierta incertidumbre. No se puede olvidar que la conservación abre las puertas a que los riesgos que se ciernen sobre la información de carácter personal, ya comentados, sigan vigentes. Estos riesgos desaparecen sólo con la supresión de los datos. Ante este hecho parece necesario encontrar alguna fórmula para garantizar que la conservación no suponga la creación de un sistema que favorezca el uso incorrecto de los datos de salud. Los principios de calidad juegan un papel

---

[3416] Artículo 20.2 Ley 3/2001, de 28 de mayo, de Galicia, reguladora del Consentimiento Informado y de la Historia Clínica de los Pacientes: "*se conservará indefinidamente la siguiente información:*
-Informes de alta; - Hojas de consentimiento informado; -Hojas de alta voluntaria; -Informes quirúrgicos y/o registros de parto; -Informes de anestesia; -Informes de exploraciones complementarias; -Informes de necropsia; -Hoja de evolución y de planificación de cuidados de enfermería; -Otros informes médicos; -Cualquier otra información que se considere relevante a efectos asistenciales, preventivos, epidemiológicos o de investigación; La información de aquellas historias clínicas cuya conservación sea procedente por razones judiciales.
3. El resto de la información se conservará, como mínimo, hasta que transcurran cinco años desde la última asistencia prestada al paciente o desde su fallecimiento".
En la Comunidad Autónoma de Valencia, la Orden de 24 de septiembre de 2001, de la Consellería de Sanidad, por la que se normalizan los Documentos Básicos de la Historia Clínica Hospitalaria de la Comunidad Valenciana y se regula su Conservación, se recogen en su artículo 4 hasta 41 documentos sanitarios diferentes que componen la historia clínica, atribuyendo a cada uno de ellos un plazo determinado de conservación.
[3417] Artículo 10 R (97) 5: "*1. en general, los datos médicos no deben conservarse más tiempo del necesario para alcanzar el propósito para el que se recogieron y procesaron; 2. cuando se acredite la necesidad de conservar los datos médicos que ya no tienen uso alguno para el fin con el que se recabaron por un interés legítimo de la salud pública o de la ciencia médica, o de la persona a cargo del tratamiento médico o del controlador del archivo en orden a permitirles la defensa en o el ejercicio de una reclamación legal, o por razones históricas o estadísticas, se adoptarán las medidas técnicas oportunas para asegurar su correcta conservación y seguridad, teniendo en cuenta la intimidad del paciente. 3. A petición del afectado, sus datos médicos deben ser eliminados, a menos que se hayan anonimizado o concurran intereses superiores y legítimos para no hacerlo, en particular los reseñados en el principio 10.2, o si existe una obligación de conservar los datos grabados".*
[3418] Informe jurídico AEPD 0551/2008.
[3419] VIGUERAS PAREDES, "La Nueva Regulación...", cit., 2002: "el párrafo segundo de ese mismo artículo 17 obliga a conservar la documentación clínica *sine die* (...)"; MÉJICA y DÍEZ, *El Estatuto del Paciente…,* cit., 2006, p. 198.
[3420] DE MIGUEL SÁNCHEZ, "Intimidad e Historia...", cit., 2003, p. 17; ALONSO OLEA, y FANEGO CASTILLO, *Comentario a la Ley…,* cit., 2003, p. 77. Resolución AEPD R/00113/2005, 22 de marzo de 2005, procedimiento TD/00399/2004.
[3421] Artículo 11 Decreto 45/1998.
[3422] MÉJICA y DÍEZ, *El Estatuto del Paciente…*, cit., 2006, p. 204.
[3423] VILLAR GOÑI, FAEDDA SANZ, LARA ECHECHIPÍA, ARAMBURU CLEMENTE, "Conservación y proceso…", cit., 2004, p. 296.

importante a la hora de interpretar lo fijado por las normas. El ordenamiento configura un marco en el que la información sanitaria puede conservarse durante un plazo indefinido de tiempo. Esta previsión ha de ser reinterpretada atendiendo a esos principios que determinan la calidad de los datos.

En primer lugar, cabe preguntarse si la historia clínica en todo caso ha de conservarse para cumplir con los fines previstos en las leyes o sólo en los casos en que haya una necesidad inmediata, real, no hipotética, de conservar esos datos con esos fines. El hecho de que la LBAP señale que los datos se conservarán "cuando" se den unas circunstancias (cuando existan razones epidemiológicas, etc*.)* da a entender que sólo en los casos en que haya una exigencia real podrán conservarse, y sólo durante el plazo en que sean necesarios. El equilibrio entre el derecho a la autodeterminación informativa y el fin que se persigue con la conservación de los datos tiene que ser justo. Cuando un sujeto no ha fallecido los motivos que podrán justificar la conservación pueden ser variados. Sin embargo, principalmente será la finalidad puramente asistencial la que justifique la conservación. Una vez fallecido, la justificación podrá ser la realización de investigaciones, estadísticas, esclarecimiento de responsabilidades, o incluso la asistencia de terceras personas. No hay que olvidar que la conservación de los datos sanitarios de una persona puede ser útil para la salvaguarda de la salud, sobre todo, de los descendientes de los pacientes[3424]. En todo caso, habrá que argumentar en cada supuesto, que se da alguna de las circunstancias citadas para justificar la conservación de los datos.

En segundo lugar, los principios de calidad sugieren que ningún dato puede conservarse más tiempo del estrictamente necesario. Así lo recuerda la normativa internacional[3425]. La LBAP también señala que la información se conservará durante el tiempo "adecuado"[3426]. Evidentemente, el problema interpretativo que se plantea es que no se sabe qué criterio habrá de seguirse para determinar cuál es el tiempo adecuado[3427]. Lógicamente, se entiende que deberá ser científico, de tal forma que sean los propios profesionales los que lo concreten[3428].

Por último, los datos que deberán conservarse serán los estrictamente necesarios para cumplir el fin que justifica dicha conservación. Independientemente del plazo previsto por las normas, sólo deberán ser guardados los datos estrictamente necesarios para cumplir dicho

[3424] SÁNCHEZ CARAZO y SÁNCHEZ CARAZO, *Protección de Datos...*, cit., 1999, p. 244: "aunque puede resultar más cómodo almacenar muchos datos "por si acaso" y trabajar con todos ellos, hay que tener en cuenta que los datos que se han de recoger deben de ser pertinentes como también han de serlo los datos con los que se trabajen"; MORENO VERNIS, "Documentación Clínica...", cit., 2002, pp. 37-47, realiza un interesante análisis sobre la necesidad de conservación de las historias clínicas;

[3425] Artículo 10 R (97) 5: *"en general, los datos médicos no deben conservarse más tiempo del necesario para alcanzar el propósito para el que se recogieron y procesaron"*. Documento Final del Grupo de Expertos en Información y Documentación Clínica, Madrid, 26 de noviembre de 1997, punto 2.6 del apartado relativo a la Información de la Historia Clínica: "La conservación de la información debe asegurarse, total o parcialmente, al menos durante el tiempo razonablemente necesario para alcanzar el propósito concreto que justificó su recogida, y que debe ser, cuando menos, aquel que, bajo un criterio médico, se establezca en el centro o área sanitaria para la asistencia del paciente en el curso de la enfermedad que justificó su creación".

[3426] Artículo 17.1 LBAP.

[3427] VIGUERAS PAREDES, "La Nueva Regulación...", cit., 2002: "La expresión tiempo adecuado es, desde luego, incorrecta. Y lo es porque se deja a un criterio poco claro (no se sabe si médico o jurídico o ambos), qué plazo deben conservarse".

[3428] COUDERT, "Tratamiento de datos…", cit., 2007, p. 353.

objetivo[3429]. Hay que hacer hincapié en que cuando sea posible esta conservación se deberá realizar manteniendo los datos de forma disociada[3430]. Cuando la finalidad sea judicial parece difícil que la información aparezca sin vincularla al titular de los datos. Por el contrario, en el caso de la investigación o los estudios epidemiológicos, así como en el de la realización de estadísticas, la disociación es en muchos casos posible y exigible.

La necesidad de limitar de alguna manera la obligación de conservar la documentación sanitaria viene motivada también por causas prácticas. Hay que tener en cuenta la dificultad organizativa que presenta esta obligación de conservar, debido a la ingente cantidad de información que se trata[3431]. Es claro que la historia clínica electrónica facilitaría esta previsión[3432]. Sin embargo, no hay que olvidar que también el almacenamiento de la información empleando las nuevas tecnologías requiere de medios y esfuerzo relevantes.

En atención a los criterios expuestos habrá que estar a cada caso para definir el plazo de conservación de los datos. Cuando la finalidad de la conservación sea la investigación, la realización de estudios epidemiológicos o de estadísticas, el plazo durante el que se podrán mantener los datos, sin que se puedan cancelar, se determinará atendiendo a criterios técnicos o científicos. Dependiendo del interés del dato para cumplir dichos fines la conservación se prolongará más o menos tiempo. En caso de que la finalidad sea la aclaración de responsabilidades no ocurre lo mismo. Por un lado está en juego el derecho a la tutela judicial efectiva que exige que se empleen todos los medios de prueba posibles, y por otro el derecho de cancelación del titular de los datos[3433]. A este respecto la LBAP dispone que la información puede conservarse "*a efectos judiciales*". Es necesario definir lo que entiende el legislador por dicho concepto[3434]. Puede entenderse que se refiere "a las acciones judiciales con motivo de la propia asistencia sanitaria"[3435], o, en un sentido más amplio, podría interpretarse que se refiere a cualquier causa en la que la historia clínica constituya un medio de prueba. Evidentemente, cuando haya causas abiertas, las historias deberán conservarse, independientemente de si se refiere a procesos motivados por la asistencia sanitaria o no. En cambio, cuando no existen causas abiertas la conservación deberá limitarse a los procesos que pudieran comenzar por

[3429] ANDÉREZ GONZÁLEZ, "Historia Clínica...", cit., 1999, Refiriéndose al cumplimiento de los fines judiciales señala que "estas razones abogan, en principio, por una conservación indefinida de las historias clínicas. Ahora bien, no se contradice con ello la posibilidad, a partir de un determinado momento (...), de conservar aquellos documentos e informes relevantes en el proceso asistencial, eliminando aquella otra documentación, normalmente voluminosa (...) sustituyéndola por la elaboración de un informe que resuma las incidencias reseñables".

[3430] Esta idea se refuerza en la reciente Ley 16/2010 de Cataluña, Artículo único.7.

[3431] MORENO VERNIS, "Documentación Clínica…", cit., 2001, p. 38; ALONSO OLEA y FANEGO CASTILLO, *Comentario a la Ley…,* cit., 2003, p. 76: señala las dificultades de los centros sanitarios para hacer cumplir la Ley cuando les obliga a conservar por tiempo, prácticamente, indefinido las historias clínicas; YUGUERO DEL MORAL, Luis, "Definición, contenido y archivo…", cit., 2004, p. 206; RODRÍGUEZ LÓPEZ, *La Autonomía del Paciente…,* cit., 2005, p. 183; TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, pp. 46-47.

[3432] VILLAR GOÑI, FAEDDA SANZ, LARA ECHECHIPÍA y ARAMBURU CLEMENTE, "Conservación y proceso…", cit., 2004, p. 303.

[3433] STS 21 de junio de 2004, FJ 2, donde se pone de manifiesto la necesidad de conservar los datos sanitarios, con el fin de salvaguardar la tutela judicial efectiva en futuros procesos judiciales en que el empleo de la información médica pueda constituir un medio de prueba. Concluye el Tribunal que no es necesario para proteger el derecho a defenderse en futuros procedimientos conservar indefinidamente toda la historia clínica de todas las personas.

[3434] ATELA BILBAO y GARAY ISASI, "Ley 41/2002...", cit., 2004, pp. 59-60, re refieren a la posible inconstitucionalidad de este precepto debido a su indeterminación.

[3435] ATELA BILBAO y GARAY ISASI, "Ley 41/2002...", cit., 2004, p. 62.

motivo de circunstancias derivadas de la asistencia sanitaria. Los principios de calidad hacen que no puedan conservarse los datos para resolver hipotéticos procesos judiciales que no tengan fundamento inminente. Si se interpretara lo contrario los datos se conservarían de manera automática por si surgiera un proceso. En todo caso, cuando el fin es el de solicitar responsabilidades judiciales a un sujeto, las acciones pueden ejercerse en plazos superiores a esos iniciales cinco años, como se ha visto al analizar el bloqueo[3436].

La situación en la que se conservan los datos dependerá también de la finalidad. En el período en que la información se conserva con fines estrictamente asistenciales, independientemente de que ese mismo documento, en ese espacio de tiempo, pueda ser empleado con otros fines como son los judiciales, epidemiológicos, de investigación o estadísticos, la historia clínica y el resto de la documentación sanitaria permanece activa en la medida en que se pueden ir introduciendo alteraciones o modificaciones en la misma. En este caso, por lo tanto, la necesidad de cumplir las garantías y derechos previstos en la normativa de protección de datos se verá reforzada. Mientras tanto, cuando este fin ha sido ya cumplido y los datos se conservan con otros objetivos como los judiciales la historia clínica no es activa sino pasiva, pues no sufre variaciones, por lo que el riesgo de que los datos puedan ser tratados de manera torticera o se produzcan perjuicios de dicha manipulación se reduce[3437]. Concretamente, cuando la finalidad sea únicamente judicial no se puede hablar de conservación sino de bloqueo, con lo que ello implica.

Resumiendo, los datos sanitarios pueden conservarse por diferentes motivos durante diversos espacios temporales. Con fines puramente asistenciales se fija un plazo mínimo de conservación que varía según la normativa, y con otros fines puede llegar a justificarse una conservación indefinida. Lo más importante será atender a los principios de calidad para determinar en última instancia el plazo concreto de conservación. Este ejercicio deberá responder a criterios científicos y deberán llevarlo a cabo los profesionales sanitarios. En esta línea, la normativa más reciente al respecto ha fijado acertadamente la necesidad de que sea, generalmente, la dirección de los centros, con el asesoramiento de un órgano encargado de la gestión de las historias clínicas, la que tome este tipo de decisiones[3438].

III.2.2.C. Referencia a algunos problemas prácticos que plantea el ejercicio del derecho de cancelación en el ámbito sanitario.

Más allá de esta perspectiva general la doctrina ha considerado diferentes problemas concretos sobre la obligación que las leyes imponen de conservar los datos sanitarios. En primer lugar, se plantea el problema que puede surgir cuando el profesional sanitario se jubila o cesa en

[3436] DE LORENZO Y MONTERO, *Derechos y Obligaciones*…, cit., 2003, p. 121: la LBAP señala que la historia clínica se conservará durante 5 años. Sin embargo, hay que tener en cuenta que, por ejemplo, para pedir la responsabilidad contractual de los profesionales sanitarios hay un plazo de prescripción de la acción de 15 años, con lo que si se han cancelado previamente dichos datos no podrán llevarse a cabo las acciones pertinentes.
[3437] Recomendación 2/2004, de 30 de julio, de la APDCM, sobre Custodia, Archivo y Seguridad de los Datos de Carácter Personal de las Historias Clínicas no Informatizadas, artículo segundo punto quinto.
[3438] Artículo único de la Ley 16/2010, 3 de junio, que modifica la Ley 21/2000, 29 de diciembre, sobre los Derechos de Información concerniente a la Salud y la Autonomía del Paciente, y la Documentación Clínica.

el ejercicio de su labor[3439]. La obligación de conservar las historias clínicas se impone en la normativa sanitaria a los centros sanitarios[3440] o a los profesionales sanitarios, en caso de que realicen su actividad de manera individual[3441]. Por lo tanto, en el supuesto de que un profesional sanitario se jubile o cese en su carrera el centro deberá conservar la historia clínica y remitirla al médico que el paciente elija. En el caso de que el profesional realice la actividad por cuenta propia, el centro cierre o, simplemente, el titular desee cambiar de centro, la solución parece que pasa porque se otorgue la historia al paciente para que la transmita al profesional que elija[3442].

En segundo lugar, se plantea la cuestión de cómo se cumple la obligación de conservar los datos cuando su tratamiento se lleva a cabo a través de un encargado, en atención a la regulación del artículo 12 de la LOPD. ¿Cabe la posibilidad de que, en caso de que exista un supuesto de acceso por cuenta de terceros a los ficheros y exista la obligación de conservar los datos, el encargado del fichero conserve la información a pesar de que haya finalizado su contrato con el responsable del fichero? Si se tiene en cuenta el articulado de la LOPD se observará que el encargado deberá devolver los datos al responsable o destruirlos una vez se haya cumplido la prestación que se le ha encargado[3443]. Parece que no corresponde al encargado del tratamiento conservar los datos más allá del plazo de vigencia del contrato que le vincula con el responsable del fichero. El encargado del tratamiento tiene que conservar los datos en la medida en que tiene la obligación de cumplir su prestación, pero no más allá de las obligaciones adquiridas[3444].

Por último, se ha cuestionado la posibilidad de cancelar las anotaciones subjetivas que los profesionales sanitarios realizan sobre los pacientes[3445]. Se ha discutido más arriba sobre las particularidades que presentan las anotaciones subjetivas, sin embargo, merece la pena realizar alguna matización a este respecto en este momento. El derecho a la cancelación responde a la necesidad de que una vez que la manipulación de los datos relativos a una persona haya cumplido su fin, estos datos sean suprimidos de forma que no quepa posibilidad alguna de que esa información sea otra vez tratada, con el riesgo de que los derechos a la intimidad, a la autodeterminación informativa, y los demás, se vean menoscabados. Por lo tanto,

[3439] COUDERT, "Tratamiento de datos…", cit., 2007, p. 354: cuando un médico deja la profesión, éste está obligado a conservar los datos durante un plazo razonable. En la práctica lo que se realizará será una cesión de datos a otro profesional.

[3440] Artículo 17.1 LOPD.

[3441] Artículo 17.5 LBAP.

[3442] ATELA BILBAO y GARAY ISASI, "Ley 41/2002…", cit., 2004, pp. 65-71: plantea el problema de lo que hay que hacer cuando el médico de un paciente se jubila o fallece. Parece que la solución adecuada sería la de dar la historia clínica al paciente para que la llevara al médico que quisiera elegir. Se plantea el problema de si la obligación de conservar las historias persistiría si cerrara una clínica privada. Se entiende que, a falta de normativa, que la mejor solución sería la misma: dar traslado de la historia a cada paciente. Artículo único de la Ley 16/2010, 3 de junio, que modifica la Ley 21/2000, 29 de diciembre, sobre los Derechos de Información concerniente a la Salud y la Autonomía del Paciente, y la Documentación Clínica.

[3443] Artículo 12.3 LOPD: "*una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento*".

[3444] Informe jurídico de la AEPD "La Conservación de los Datos por el Encargado del Tratamiento", nº 283/2004, 2004, en http://www.agpd.es

[3445] ESTEBAN, "Las Notas Personales...", cit., 2002, recoge las palabras de J. M. FERNÁNDEZ LÓPEZ, en este sentido.

independientemente de a quién se le atribuya la propiedad sobre dichas anotaciones, parece evidente que este fin no se cumple si las anotaciones subjetivas con referencia a un paciente determinado perduran en el tiempo. En todo caso, de conservar este tipo de aclaraciones u opiniones, deberían permanecer con carácter disociado. La conservación de estas anotaciones de forma asociada sólo podrán justificarse con las finalidades que señalan las normas y durante los plazos marcados por éstas.

IV. DERECHO DE OPOSICIÓN.

IV.1. La incorporación del derecho de oposición en la LOPD.

En la actualidad el ordenamiento reconoce expresamente el derecho de oposición. La LOPD señala que "*en los casos en que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado*"[3446]. Señala la Ley que el procedimiento para ejercer este derecho, como ocurre con los derechos de acceso, cancelación y rectificación, será determinado reglamentariamente y que, en cualquier caso, no se exigirá contraprestación para su ejercicio[3447]. La norma estatal regula también un supuesto concreto en que puede alegarse el derecho de oposición. Concretamente, dispone que podrá llevarse a cabo esta facultad, previa petición y sin gastos, en los tratamientos de los datos que tienen como fin la publicidad y prospección comercial, teniendo como efecto la cancelación inmediata de dichos datos[3448]. Esta regulación viene a recoger en el ámbito interno lo ya dispuesto en la Directiva europea[3449]. Sin embargo, parece que la norma estatal tiene un ámbito de aplicación más amplio. En la Directiva la oposición tiene aplicación, de inicio, en supuestos concretos, vinculados sobre todo a

[3446] Artículo 6.4 LOPD.
[3447] Artículo 17 LOPD.
[3448] Artículo 30 LOPD: "*1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mimos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento*". "*4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud*".
[3449] Considerando 45 Directiva 95/46/CE: "*Considerando que cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo, tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales concretas".* Artículo 14 Directiva 95/46/CE*: "Derecho de oposición del interesado. Los Estados miembros reconocerán al interesado el derecho a:*
a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos;
b) oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernen respecto de los cuales el responsable prevea un tratamiento destinado a la prospección ; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente el derecho de oponerse, sin gastos, a dicha comunicación o utilización.
Los Estados miembros adoptarán todas las medidas necesarias para garantizar que los interesados conozcan la existencia del derecho a que se refiere el párrafo primero de la letra b)".

situaciones en que los datos son tratados por las administraciones. En cualquier caso, la norma europea deja la puerta abierta a que se pueda aplicar a más casos que los expresamente previstos[3450]. Por el contrario, en la norma estatal la oposición parece aplicarse a todos los casos en que no sea necesario el consentimiento del afectado para llevar a cabo el tratamiento de datos. La escueta regulación de la Ley se completa con la llevada a cabo por el reglamento que la desarrolla[3451]. El RDLOPD combina los diferentes supuestos reconocidos en la norma estatal y europea[3452], y desarrolla la fórmula que ha de emplear el interesado para ejercer la oposición[3453]. La jurisprudencia y las resoluciones de la AEPD no se han pronunciado en demasiadas ocasiones sobre el contenido de este derecho. Lo cierto es que no se trata de una facultad de común aplicación, debido principalmente a la necesidad de demostrar un motivo fundado y legítimo que justifique su ejercicio. Esta circunstancia no es óbice para hacer un breve análisis sobre las características principales del derecho de oposición, pues se trata de una facultad que cada vez está encontrando un mayor campo de acción[3454].

La LOPD reconoce la genérica facultad de oponerse a los tratamientos que inicialmente no exigen del consentimiento de su titular, en caso de que se demuestren motivos suficientes para ello. Se trata de un derecho que no aparecía reconocido expresamente en la anterior LORTAD y, por lo tanto, de nueva incorporación en la actual LOPD, una norma que no contiene exposición de motivos y que no explica la razón de ser de este derecho. En algún caso se había planteado por la doctrina que el derecho de oposición ya se encontraba en la anterior LORTAD en la

[3450] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 160: se refiere en relación al derecho de oposición en la Directiva europea, a la expresión "al menos", que da a entender que puede reconocerse el derecho en más supuestos.

[3451] GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, pp. 304-305: habla de la oscuridad en la regulación de la LOPD del derecho de oposición; PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 319. habla de la falta de regulación de la oposición en al LOPD.

[3452] Artículo 34 RDLOPD: "*El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos: a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario; b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación; c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento*".

[3453] Artículo 35 RDLOPD: "*1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.*
Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse contar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.
2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máimo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.
En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite si derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo".

[3454] Resolución AEPD R/02675/2009, 21 de enero de 2010, procedimiento TD/00999/2009: En esta resolución se pone de manifiesto que el alcance del derecho de oposición es grande, pues se admite la posibilidad de ejercer el derecho de oposición a un tratamiento por parte de Google, para que evite que los datos referentes a una persona concreta puedan ser accesibles en el buscador.

referencia que "permitía al afectado negarse a facilitar un dato de carácter personal en el caso de que no fuese obligatorio hacerlo cuando se le tenía que informar del carácter obligatorio o facultativo de su respuesta a las preguntas que le fueran planteadas"[3455]. En esta misma línea, en el ordenamiento autonómico se ha previsto en algún caso la aplicabilidad del derecho de oposición, más allá de en los supuestos reconocidos en la LOPD, cuando el tratamiento de dicha información sí requiere el consentimiento[3456]. Tanto en la anterior LORTAD, como en el citado decreto autonómico, los supuestos a los que se ha hecho referencia conciernen a casos en que el titular no está obligado a dar la información. En estos supuestos el titular de los datos tiene la potestad de elegir si quiere que los datos sean o no tratados. Se entiende que el derecho de oposición no se refiere a estos casos, sino que concierne a circunstancias en que, *a priori,* el tratamiento de esos datos está legitimado y puede llevarse a cabo sin el consentimiento del titular, si bien, debido a determinadas razones de peso, este tratamiento, en principio legitimado, puede paralizarse y rechazarse por el titular de los datos[3457]. La oposición, como derecho, para ser efectiva, requiere de un motivo fundado y legítimo vinculado a una concreta situación personal, exigencia que carecería de sentido en caso de que se admitiese la oposición cuando el consentimiento del titular es requerido, pues el consentimiento puede otorgarse o no independientemente de la naturaleza de los motivos que conduzcan a ello.

La inclusión de este derecho en la LOPD responde a dos motivos fundamentales. En primer lugar, a la evidente necesidad de trasponer la Directiva europea. En segundo lugar, y desde un punto de vista sustantivo, la inclusión se justifica porque la oposición viene a reforzar la capacidad del titular de los datos de controlar lo que sucede con los mismos. En la medida en que supone la facultad de rechazar un tratamiento determinado de sus datos en supuestos, además, en que no es necesario el consentimiento del titular, parece evidente que constituye una herramienta más para decidir sobre la información concerniente a cada uno. Si se ejerce el derecho de oposición y aún así se continúa con un tratamiento de datos se estará vulnerando el derecho a la autodeterminación informativa.

Podría parecer que en la LOPD, al ser las citas al derecho de oposición tan escasas, es tratada esta facultad como derecho de segundo orden. A esta misma conclusión podría llevar

[3455] Artículo 5 LORTAD. DEL PESO NAVARRO, *Ley de Protección...*, cit., 2000, p. 55.

[3456] Artículo 5 Decreto 308/2005, de 18 de octubre de 2005, por el que se desarrolla la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de creación de la Agencia Vasca de Protección de Datos: "*1. Cuando el tratamiento de datos de carácter personal requiere el consentimiento inequívoco del afectado, el derecho de oposición se ejerce tanto mediante la no manifestación de dicho consentimiento como mediante la manifestación de la negativa a concederlo.*
2. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de datos de carácter personal, y siempre que la ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal, mediante escrito dirigido al responsable del fichero. En tal supuesto, éste excluirá del tratamiento o tratamientos a que se refiera la petición, los datos relativos al afectado y le notificará a éste, en un plazo no superior a diez días, los términos en los que se ha efectuado la exclusión".

[3457] DAVARA RODRÍGUEZ, *Manual de Derecho...,* cit., 2005, p. 79: "no representa este derecho que la negativa del afectado al tratamiento automatizado de sus datos de carácter personal impida dicho tratamiento, sino el derecho a oponerse a dicho tratamiento, por razones legítimas propias de su situación particular salvo cuando la legislación nacional disponga otra cosa".

alguna consideración que realiza la Directiva europea al respecto de este derecho[3458]. Y es que de la redacción de esta norma puede desprenderse fácilmente que el reconocimiento del derecho de oposición en los ordenamientos estatales es voluntario. Tras regular el derecho de oposición, la Directiva dispone en dos ocasiones que los Estados miembros podrán aprobar regulaciones contrarias a la configurada en la norma europea[3459]. Podría entenderse de esta normación que se faculta a los Estados miembros a no reconocer el derecho de oposición.

Sin embargo, lo cierto es que la relevancia de este instrumento no es menor en la práctica que la de los demás derechos de la persona. Se considere como figura vinculada al consentimiento o como derecho de la persona, más cercano a los derechos de acceso, cancelación, etc., el hecho de que la oposición no haya obtenido una amplia regulación en la LOPD no ha de llevar a deducir que se está ante un derecho de segundo orden. El derecho de oposición se erige en una facultad de importancia para el control de los datos de carácter personal[3460]. Con la inclusión de este derecho se quieren limitar, de alguna manera, los amplios ámbitos que reconoce la Ley para el tratamiento de los datos de carácter personal sin necesidad del consentimiento del titular. Fundamentalmente, se entiende que se pretende limitar la potestad que la LOPD otorga a la Administración a la hora de tratar los datos de carácter personal sin el consentimiento del titular[3461]. Ya se ha visto que las administraciones cuentan con cierto privilegio a la hora de manipular la información de carácter personal. El derecho a oponerse constituye un límite a dicho privilegio, si bien es cierto que su aplicabilidad en el sector público es en la práctica limitada, debido a que no es fácil justificar la oposición cuando lo que está en juego es el interés público[3462].

IV.2. Problemas de interpretación en relación al derecho de oposición y su aplicabilidad en el ámbito sanitario.

El derecho de oposición plantea diferentes problemas de interpretación. Probablemente se esté en estos momentos ante el derecho que mayores incógnitas presenta de los que aquí se analizan.

A) En primer lugar, es cuestionable su ubicación en la LOPD. Si se atiende a la estructura de la Ley, se observará que su regulación no se encuentra junto a los demás derechos de la persona, sino en el apartado correspondiente al consentimiento, lo cual genera cierta confusión[3463]. Esta desvinculación entre el derecho de oposición y los derechos al acceso, rectificación o cancelación se produce, por ejemplo, en los artículos 23 y 24 de la LOPD, que al

[3458] HEREDERO HIGUERAS, *La Directiva...*, cit., 1997, p. 154: "El <<Considerando>> 45º precisa (...) que los Estados miembros no están obligados a reconocer este derecho".
[3459] Considerando 45 y artículo 14 Directiva 95/46/CE.
[3460] DE MIGUEL SÁNCHEZ, *Tratamiento de Datos*..., cit., 2004, p. 56, refiriéndose al derecho de oposición señala que ello "supone un importante impulso para el control ejercido por el particular sobre el uso de su información personal".
[3461] MARTÍN-CASALLO LÓPEZ, "Derechos de acceso...", cit., 2000: "su finalidad va dirigida a servir de contrapeso a las facultades que se reconocen tanto a la autoridad pública como a los particulares de la posibilidad de que estos efectúen lícitamente un tratamiento de datos".
[3462] FERNÁNDEZ SALMERÓN, *La Protección de los datos*..., cit., 2003, p. 351.
[3463] HERRÁN ORTIZ, *El Derecho a la Intimidad...,* cit., 2002, p. 224; CONDE ORTIZ, *La Protección de Datos...,* cit., 2005, p. 88.

regular las excepciones aplicables a los derechos se refieren únicamente a los de acceso, rectificación y cancelación, sin hacer mención a la oposición. Se entiende aquí que no es totalmente desacertada la situación del derecho en este apartado.

De inicio podría entenderse que el derecho de oposición, como derecho, debería haber sido reconocido expresamente en un apartado propio en el Titulo III de la LOPD relativo a los Derechos de las Personas, pues es evidente que esta facultad constituye también un instrumento activo de control para el titular de los datos[3464]. Sin embargo, si se atiende a su contenido se podrá concluir que el reconocimiento del derecho de oposición en el Título II, junto al derecho a otorgar el consentimiento, no carece de fundamento. Esto se debe a que la oposición y el consentimiento son figuras íntimamente relacionadas[3465], en la medida en que los efectos de la revocación del consentimiento y del ejercicio del derecho a la oposición son idénticos. El consentimiento es la autorización para llevar a cabo un tratamiento, y su revocación supone simplemente la declaración de voluntad del titular de los datos denegando el consentimiento otorgado. La oposición conlleva los mismos efectos, pero vinculado a los casos en que el derecho a otorgar el consentimiento resulta exceptuado. El derecho de oposición, por lo tanto, si bien aparece relacionado a los derechos clásicos que componen el *habeas data*, como son el acceso, la cancelación y la rectificación, por cuanto constituye una facultad subjetiva de control de la información de carácter personal, aparece también relacionado a la figura del consentimiento, en la medida en que constituye una fórmula para limitar la capacidad de tratamiento de aquéllos que tienen la posibilidad de manipular dichos datos sin necesidad de recabar la autorización de su titular.

B) En segundo lugar, desde el punto de vista práctico, resulta problemática la previsión de ciertos requisitos y la fijación de determinados límites a la hora de ejercer el derecho de oposición. Primero, la LOPD apunta que se reconoce este derecho "*siempre que una ley no disponga lo contrario*"[3466]. Según esta regulación ¿bastaría con que el tratamiento de unos datos esté autorizado por una ley para que el derecho de oposición se vea exceptuado, o es necesario que la Ley fije expresamente la excepción para el derecho a la oposición arguyendo intereses superiores? La previsión del artículo 6.4 de la LOPD reproduce parcialmente en este punto lo que señala el artículo 6.1, referido al derecho a otorgar el consentimiento, que dispone que el tratamiento de los datos de carácter personal requerirá del consentimiento del titular "*salvo que la ley disponga otra cosa*". Cabe decir, por lo tanto, lo mismo que se decía al analizar este último precepto: no es suficiente con que una ley habilite un tratamiento determinado de datos, sino que es necesario que ese tratamiento responda a intereses de relevancia suficiente y que la ley recoja la excepción al derecho a la oposición de forma expresa o que esta excepción sea deducible, en la medida en que el tratamiento se entiende obligatorio para la consecución de un fin. Como ya se ha apuntado en numerosas ocasiones, las excepciones a los derechos

[3464] DAVARA RODRÍGUEZ, *Manual de Derecho...,* cit., 2005, p. 79, entiende que el derecho de oposición "debería haber sido objeto de estudio independiente y no introducirse en un artículo en el que se regula el consentimiento y sus excepciones". Considera este autor que el derecho de oposición "ni se encuentra bien recogido en la LOPD (...) ni está en el lugar adecuado"; CONDE ORTIZ, *La Protección...*, cit., 2005, p. 88.

[3465] SAN 17 de abril de 2007, FJ 3, en la que se refiere a la oposición como complemento indispensable del consentimiento. VILLAVERDE MENÉNDEZ, "Derecho de oposición…", cit., 2010, pp. 496-498.

[3466] Artículo 6.4 LOPD.

fundamentales tienen que fijarse de manera precisa y expresa, de tal forma que no generen inseguridad.

Segundo, la normativa exige para poder ejercer la oposición, que se argumente por parte del titular de los datos un motivo fundado y legítimo relativo a una concreta situación personal. No es fácil interpretar lo que el legislador ha querido dar a entender con esta expresión por lo que habrá que ir supuesto por supuesto analizando si se esgrime un motivo suficiente. En todo caso, habrá que entender que se tiene que tratar de motivos o intereses más importantes que los que justificaron el tratamiento sin el consentimiento del titular.

Como ha apuntado la doctrina, el problema deriva del hecho de que la oposición se ejerce cuando el consentimiento resulta exceptuado. Cuando se exceptúa el derecho a consentir un tratamiento será porque hay una finalidad que justifica la aplicación de la excepción[3467]. Para justificar la oposición a un tratamiento en que se exceptúa el consentimiento, el motivo que debería esgrimir el titular de los datos a la hora de oponerse al tratamiento debería ser, en todo caso, de mayor entidad que dicha finalidad que justifica la excepción. No es fácil imaginar una tal situación. Se entiende aquí, que lo habilitado por el legislador no es otra cosa que una vía para que en cada caso concreto se pueda analizar una circunstancia particular en orden a justificar dicha oposición[3468]. No sólo se dará la oposición cuando los datos han sido recabados de fuentes accesibles al público y se emplean sin el consentimiento inicial con fines publicitarios, casos en que parece sencillo argumentar un motivo suficiente y que aparecen expresamente recogidos en la LOPD[3469]. La oposición puede llevarse a cabo, de inicio, en cualquier situación en que se justifica un tratamiento sin necesidad de autorización, atendiendo a las circunstancias particulares de la situación y a los motivos que presenta el titular de los datos.

En relación a este punto, de las normas parece desprenderse que será el responsable del fichero quien determinará si ese motivo que justifica la oposición se produce o no en la realidad[3470]. Este hecho ha de ser criticado debido a que el responsable no es un agente externo a la relación con el titular de los datos[3471]. La ponderación entre los bienes que podrían chocar en el ejercicio de esta facultad debería realizarla un órgano independiente a la relación entre las

[3467] APARICIO SALOM, *Estudio sobre la Ley...*, cit., 2000, p. 141: "parece más lógico inclinarse por una definición más genérica del derecho de oposición de la que se deriva de los dos preceptos de la LOPD en que se emplea el término derecho de oposición, en el sentido de incluir en dicho concepto el rechazo del interesado al uso de los datos, ya sea general, oponiéndose al tratamiento, ya sea a algún uso determinado, oponiéndose a alguna finalidad específica o la cesión de los datos"; GUICHOT, *Datos Personales...*, cit., 2005, pp. 396-397, se decanta por un concepto restringido del derecho de oposición. Si el derecho de oposición se refiere a los casos en que no se exige consentimiento del titular para el tratamiento, no tiene sentido que la oposición se refiera a la finalidad, pues es ésta precisamente la que motiva que no se requiera consentimiento, y si se acepta la teoría de APARICIO se desvirtúa la esencia misma de la oposición. En caso de que el rechazo a la finalidad se refiriese a los supuestos en que es necesario el consentimiento, no sería oposición sino, como dice GUICHOT consentimiento condicionado.

[3468] VILLAVERDE MENÉNDEZ, "Derecho de oposición…", cit., 2010, p. 500, apunta que el ejercicio del derecho de oposición lleva a la aplicación estricta del principio de proporcionalidad entre los diferentes intereses que puedan entrar en juego.

[3469] Artículo 30.4 LOPD.

[3470] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 325: ha de ser el responsable del fichero quien determine si el titular de los datos presenta motivos fundados para ejecutar la oposición.

[3471] GUERRERO PICÓ, *El impacto de Internet…,* cit., p. 306: la oposición se dará cuando haya un motivo fundado y legítimo. La autora critica el hecho de que pueda ser el responsable el que decida si exista esa causa o no.

personas implicadas en el tratamiento de datos. En todo caso, al igual que ocurría con el acceso, cancelación o rectificación, el titular de los datos podrá acudir a la agencia de protección de datos correspondiente en caso de que el responsable del fichero deniegue el ejercicio de la oposición[3472].

El derecho a la oposición se entiende, por lo tanto, como derecho a negarse a que un tratamiento en el que no se requiere del consentimiento del titular de los datos siga adelante. En el momento en que el titular tiene conocimiento del tratamiento puede ejercer el derecho. En este sentido, es importante señalar que el derecho a recibir información también obliga a informar al titular de los datos sobre el derecho a oponerse al tratamiento.

C) En tercer lugar, de un análisis comparativo se plantea un problema de interpretación en relación a los supuestos en que se aplica la oposición. La Directiva europea parece reducir los casos en que se puede ejercer el derecho a unos supuestos limitados, frente al reconocimiento general que realiza la LOPD[3473]. Esta aparente contradicción se resuelve si se tiene en cuenta la amplitud de los conceptos empleados en la norma europea a la hora de regular la oposición. La Directiva se refiere a la posibilidad de ejercer el derecho cuando el tratamiento se justifica por tener como fin el cumplimiento de una misión de interés público o inherente al ejercicio del poder público, o por dirigirse a la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero a quien se comunican los datos. El uso en la normativa europea, tanto en su articulado como en sus considerandos, de conceptos tan amplios como "tratamiento que atiende a razones de interés público" o "del ejercicio de autoridad pública", o "interés legítimo de una persona física" [3474], hace que el derecho de oposición sea aplicable a prácticamente todo tratamiento en que no es necesario el consentimiento del titular de los datos. Hay que recordar, además, que el empleo de la expresión "al menos" para referirse a los casos en que se puede ejercitar el derecho de oposición, refuerza la idea de que el derecho puede ser aplicable a todos los supuestos en que no es exigible el consentimiento del titular, pues indica que a las situaciones a las que la Directiva hace referencia se les pueden añadir otras.

Por último, el procedimiento a seguir en el ejercicio del derecho no plantea mayores problemas. Las normas que antes de la entrada en vigor del RDLOPD desarrollaban la LORTAD no se referían a la oposición. Era normal por cuanto que la anterior Ley de protección de datos no reconocía expresamente este derecho. Esta regulación planteaba el problema de que cuando

[3472] Artículo 44.3 LOPD: "*Son infracciones graves: e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada*". Informe jurídico AEPD 0291/2009: el ejercicio del derecho de oposición se ha puesto de manifiesto en ocasiones en relación al supuesto común en que se remite publicidad a los ciudadanos. La oposición a dicho tratamiento de sus datos conlleva automáticamente que la continuación en la remisión de dicha publicidad constituya un tratamiento contrario a la LOPD.

[3473] HEREDERO HIGUERAS, *La Directiva Comunitaria…,* cit., 1997, p. 153; HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 224: "si la Directiva particulariza los supuestos en los que será posible oponerse al tratamiento (...), la ley española opta por establecer un derecho de oposición general".

[3474] Considerando 45 y artículo 14 Directiva 95/46/CE.

entró en vigor la LOPD la normativa que desarrollaba la LORTAD seguía vigente, con el obstáculo de que estos reglamentos no regulaban el ejercicio de la oposición[3475].

El RDLOPD regula expresamente la forma en que ha de ejercerse este derecho sin plantear mayores problemas de interpretación. El titular de los datos deberá formalizar una solicitud que se dirigirá al responsable del tratamiento. La solicitud deberá incluir los motivos que justifican el ejercicio del derecho. El responsable deberá resolver la solicitud en el plazo de diez días, a contar desde que recibió la solicitud. Cuando el responsable no cuente con información sobre el titular tendrá igualmente la obligación de contestar. El responsable, cuando estime la solicitud deberá excluir los datos del tratamiento. En caso de que desestime la oposición deberá contestar motivando la denegación. Si el responsable no contesta en plazo o deniega la solicitud, el titular de los datos podrá acudir a la agencia de protección de datos correspondiente para solicitar la tutela de dicho organismo[3476].

En el ámbito estrictamente sanitario el ordenamiento no hace ninguna referencia al ejercicio del derecho de oposición. Su aplicabilidad en este sector habrá que deducirla, por lo tanto, de la interpretación conjunta de la normativa de protección de datos y la normativa sanitaria. Se puede adelantar desde ahora que el derecho de oposición no es fácilmente aplicable aquí[3477]. En principio, y partiendo de la consideración de que los datos de carácter personal sanitarios son manipulables sin el consentimiento del titular en determinadas circunstancias, el derecho que se analiza podría ser perfectamente aplicable. Sin embargo la LOPD apunta también que la oposición se aplicará salvo que una Ley disponga lo contrario. La LBAP no dice nada sobre el derecho de oposición de los ciudadanos. Sin embargo, la obligación de conservar los datos sanitarios durante determinado plazo de tiempo es indicativo de que el ciudadano no podrá oponerse a que sus datos sanitarios sean tratados[3478]. Resulta prácticamente imposible encontrar algún motivo lo suficientemente legítimo y razonado que justifique el derecho de oposición en estos casos[3479]. Otra cosa será fuera de estos casos en que la conservación es obligatoria. Se ha visto que la obligación de conservar no entra en juego en todo caso. Cuando no exista esta

[3475] Memoria de la AEPD 2003, p. 53: "han podido suscitarse dudas sobre la plena efectividad de este derecho, por una posible ausencia de desarrollo reglamentario"; Resolución AEPD nº R/00558/2004, procedimiento TD/00185/2004, 20 de octubre de 2004.
[3476] Artículo 35 RDLOPD.
[3477] MUNAR BERNAT, "El Tratamiento...", cit., 1997, p. 125: "En el supuesto de los datos médicos, no parece tener mucho sentido ese derecho, por cuanto estamos partiendo de la base de que se le ha solicitado el consentimiento para el tratamiento de sus datos, o a través de una norma general se ha establecido el derecho del responsable del tratamiento para proceder en todo caso al mismo". TRONCOSO REIGADA, *Protección de Datos…,* cit., 2008, p. 55: la oposición tiene poco recorrido en la práctica sanitaria debido a la finalidad que se persigue en este sector; LARIOS RISCO, "La historia clínica…", cit., 2009, p. 177.
[3478] Código tipo de tratamiento de datos de carácter personal para odontólogos y estomatólogos de España, diciembre 2009: En relación a la oposición, expresamente se señala que este derecho podrá ejercerse siempre y cuando no vaya en detrimento de la prestación de asistencia sanitaria.
[3479] SÁNCHEZ CARO y ABELLÁN, *Telemedicina y protección…,* cit., 2002, p. 77: en el ámbito sanitario no será normal el ejercicio de la oposición. Pero si se ejerciera podría rechazarse en beneficio de bienes jurídicos de mayor entidad; TRONCOSO REIGADA, *Guía de Protección...*, cit., 2004, p. 32: "de producirse dicha oposición, podría evidentemente ser rechazada en aplicación de un criterio de primacía del derecho a la vida frente al derecho a la intimidad".

obligación la oposición tiene plena cabida[3480]. En general, habrá que atender a los casos concretos para observar qué fines justifican la conservación de los datos y qué motivos presenta el titular de los datos para oponerse a la manipulación concreta.

V. DERECHO A IMPUGNAR VALORACIONES.

La LOPD reconoce el derecho a no verse sometido a una decisión con efectos jurídicos sobre el titular de los datos o que le afecte de manera significativa, que se fundamente exclusivamente en una manipulación de datos que tiene como fin evaluar aspectos de su personalidad[3481]. En esta misma línea, la norma señala que dicho titular tendrá el derecho a impugnar los actos administrativos o decisiones privadas dirigidas a valorar su comportamiento y que se basan únicamente en un tratamiento de datos de carácter personal de la que resulte una definición de sus características personalidad[3482]. En estos casos el titular de los datos tendrá derecho a obtener información sobre los criterios de valoración y el programa de tratamiento empleados para adoptar la decisión que le ha afectado[3483].La Directiva europea recoge también, cuando regula la oposición, este derecho a no verse sometido a decisiones adoptadas apoyándose únicamente en tratamientos de datos que tienen como objetivo evaluar determinados aspectos de la personalidad del titular. Sin embargo, reconoce unos supuestos en que este derecho se ve limitado: cuando una ley así lo establezca, o cuando la decisión que afecta al titular de los datos se ha adoptado en el marco de un contrato, siempre y cuando se reconozca la posibilidad al titular de los datos de defender su postura a la hora de valorar su personalidad[3484]. La norma europea prevé también la facultad del titular a conocer cómo se han realizado dichas valoraciones, si bien dicho acceso tiene como límite el derecho a la propiedad intelectual o derechos de autor sobre los programas utilizados para realizar las valoraciones[3485].El reglamento

[3480] NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, p. 193: La LBAP señala que la HC tiene que contar con una serie de datos. Sobre estos datos es difícil ejercer la oposición. Fuera de estos datos que obligatoriamente han de encontrarse en la HC sí podría ejercerse el derecho de oposición.

[3481] Artículo 13.1 LOPD:

[3482] Artículo 13.2 LOPD:.

[3483] Artículo 13.3 LOPD.

[3484] Artículo 15 Directiva 95/46/CE. "*1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinados a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. 2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguarda de su interés legítimo; b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado"*.

[3485] Considerando 41 Directiva 95/46/CE: "*Considerando que cualquier persona debe disfrutar del derecho de acceso a los datos que le conciernan y sean objeto de tratamiento, para cerciorarse, en particular, de su exactitud y de la licitud de su tratamiento; que por las mismas razones cualquier persona debe tener además el derecho de conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan, al menos en el caso de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15, que este derecho no debe menoscabar el secreto de los negocios ni la propiedad intelectual y en particular el derecho de autor que proteja el programa informática; que no obstante esto no debe suponer que se deniegue cualquier información al interesado*".

que desarrolla la Ley estatal reproduce básicamente, también en el apartado dedicado al derecho a la oposición, la regulación realizada por la norma europea[3486].

Este derecho se relaciona directamente con el principal riesgo que las TIC generan para al Derecho a la autodeterminación informativa, que no es otro que el aumento de posibilidades de crear perfiles completos de los ciudadanos mediante el almacenamiento masivo de datos de carácter personal, y el consiguiente tratamiento de los mismos[3487]. Es conocido cómo en determinados sectores, caso del bancario, se crean perfiles que valoran la capacidad crediticia de las personas partiendo de tratamientos de datos concretos[3488]. La propia jurisprudencia ha puesto de manifiesto en alguna ocasión la existencia de sistemas de tratamiento de datos, como el *scoring,* que se dirigen a valorar determinados aspectos de la vida de una persona, valoraciones que, a su vez, sirven como fundamento para tomar decisiones[3489]. Efectivamente, como se señalaba en el capítulo primero, las nuevas tecnologías permiten que cantidades inimaginables de datos se transmitan por las redes y que se almacenen en ficheros con una capacidad hasta ahora desconocida. Sin embargo, el verdadero riesgo para el derecho a la autodeterminación informativa, no es tanto esta capacidad de almacenamiento, sino la posibilidad de que todos estos datos se relacionen entre sí, para deducir así perfiles completos de los ciudadanos[3490]. La posibilidad de que partiendo de este cruce de datos relativos a un ciudadano puedan resultar valoraciones referidas a dicha persona y que basándose en esas valoraciones se tomen decisiones que afecten a los titulares de esos datos plantea muchas interrogantes.

A) Cuando se habla del derecho a impugnar determinadas decisiones hay que contextualizar su alcance. No se trata de negar la posibilidad de que se lleven a cabo valoraciones, ni que éstas puedan suponer un apoyo a la hora de tomar decisiones que afecten al titular de los datos. Lo que se niega es la posibilidad de que estas valoraciones constituyan el único fundamento a la

[3486] Artículo 36 RDLOPD: "*1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta; 2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando decisión: a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato. b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado*".

[3487] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 336: en relación al derecho de impugnar valoraciones… el tratamiento de datos puede traer perfiles o configurar determinada fama que puede valorarse positiva o negativamente (de comprar libros puede desprenderse una ideología…); SERRERA COBOS, "Derecho de impugnación…", cit., 2007.

[3488] RUIZ CARRILLO, *La Protección de los Datos…,* cit., 2001, p. 78.

[3489] SAN 15 de noviembre de 2002, FJ 1: Euskaltel contrata a una empresa con la finalidad de que realice para la primera una labor de scoring: "consistente en efectuar una valoración del riesgo según los parámetros establecidos y en emitir un resultado de apto o no apto de los clientes".

[3490] RUIZ CARRILLO, *La Protección...*, cit., 2001, p. 78: "Los <<perfiles>> son adjetivos resultantes de los cruces de información y sirven para aplicaciones publicitarias, de investigación, de <<marqueting>> y, en ocasiones, para catalogar a la persona"; DEL PESO NAVARRO, "Impugnación de valoraciones...", cit.,: "lo peligroso (...) es que nuestros datos estén almacenados en una gran base de datos y a partir de ahí se puedan obtener, transmitir, vender, etc. perfiles y se puedan hacer valoraciones muy completas de nuestra persona".

hora de tomar esas decisiones[3491]. Hay que tener en cuenta que se está hablando de que de un tratamiento de datos se deduzcan valoraciones con el componente subjetivo que de ello se deduce[3492].

B) El objetivo de la regulación lo constituye evitar que se puedan tomar decisiones perjudiciales y, sobre todo, discriminatorias, basadas en meras valoraciones. En dos preceptos la LOPD determina el sentido de este derecho. Se entiende aquí que las distintas disposiciones están relacionadas y que requieren de una interpretación conjunta. En el primero, el legislador pretende evitar que se puedan tomar decisiones "*con efectos jurídicos*" para el titular de los datos o que le "*afecten de manera significativa*". Se entiende aquí que, en general, se trata de prevenir que se puedan adoptar decisiones perjudiciales para el titular. A pesar de que la LOPD se refiera a "*decisiones con efectos jurídicos"* o "*que les afecte de manera significativa"*, se puede interpretar que lo que el legislador trata de evitar son, en general, las decisiones perjudiciales para el titular de los datos, pues cuando se trate de beneficiosas, o simplemente no perjudiciales, no parece tener sentido hablar de impugnación[3493]. Plantea cierta confusión el que se distingan las decisiones que conllevan efectos jurídicos y las que afectan de manera significativa[3494]. Y es que en la práctica las decisiones que afectan al ciudadano de manera significativa difícilmente no acarrearán efectos jurídicos. Tampoco hay que entender el calificativo de "significativa", como una forma de exigir una especial gravedad en la manera de afectar la decisión al titular de los datos[3495]. Se entiende que simplemente será necesaria la existencia de una decisión que perjudique al afectado. El perjuicio puede derivar en una afección, por ejemplo, al derecho al honor de la persona sobre la que se realiza la valoración[3496].

En el segundo, se prohíben las decisiones basadas únicamente en tratamientos de datos dirigidos a valorar el comportamiento, las características y personalidad de los sujetos[3497]. Plantea especiales dificultades determinar lo que se entiende por "*comportamiento"* o "*aspectos de su personalidad"*. En este sentido aclara estas dudas la redacción prevista en la Directiva europea o el RDLOPD en la que se hace referencia, a modo de ejemplo, a cualidades de la

[3491] NICOLÁS JIMÉNEZ, *La Protección Jurídica…,* cit., 2006, p. 189: subraya la importancia del derecho a impugnar valoraciones, pues se protege así de visiones reducciones que pretenden tomar decisiones sobre personas basándose exclusivamente en valoraciones peligrosas. El derecho se aplica a la decisión, no a la elaboración del perfil. Sin embargo, la elaboración de perfiles sí podría constituir una intromisión del honor de la Ley 1/1982. Este derecho no evita que la elaboración de perfiles y las valoraciones puedan constituir un apoyo en la toma de decisiones; LÓPEZ DEL MORAL ECHEVERRÍA, "Impugnación de valoraciones…", cit., 2010, p. 1.131.

[3492] GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 129, llama la atención sobre el riesgo de que las valoraciones que se puedan extraer de un tratamiento de datos puede no coincidan con la realidad.

[3493] HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 162, se refiere al caso del marketing directo, que se lleva a cabo seleccionando destinatarios a través del cruce de datos por ordenador, "lo que facilita la tarea de formar listados o relaciones de destinatarios con fines de publicidad directa", pero que no puede entenderse que conlleve efectos perjudiciales, por lo que no justifica la impugnación.

[3494] FREIXAS GUTIERREZ, *La Protección…*, cit., 2001, pp. 182-183.

[3495] VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, p. 186; GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, p. 290: Se podrá impugnar cuando la decisión produzca "efectos jurídicos". Hay que interpretarlo en sentido amplio: "toda aquella que incida en el ámbito de actuación de los ciudadanos".

[3496] GAY FUENTES, *Intimidad y Tratamiento…,* cit., 1995, p. 85: se ha planteado que la posibilidad de impugnar las valoraciones constituye también un instrumento para proteger el honor de las personas, por cuanto que la creación de un perfil y valorarlo puede dar una imagen errónea de la persona.

[3497] Artículos 13.1 y 2 LOPD.

persona tales como "*su rendimiento laboral, crédito, fiabilidad, conducta, etc.*"[3498]. Parece que con estas citas se trata de reconocer un amplio ámbito de aplicación a este derecho[3499]. Hay quien considera que la cita realizada por la Directiva a estos concretos casos es negativa, siendo preferible la fórmula indefinida reconocida por la LOPD[3500]. Se entiende aquí que la previsión de la Directiva es más clarificadora que la reconocida en la Ley estatal. Las referencias al ámbito laboral, etc. no constituyen una lista cerrada, sino que tienen un carácter de ejemplo como se deduce del empleo en la norma europea del término, "etc.". Lo que se trata de evitar, por lo tanto, es que analizando una serie de datos referentes a la persona puedan sacarse conclusiones sin un fundamento riguroso y que, partiendo de esas conclusiones, el responsable de los datos tome unas decisiones que puedan perjudicar al ciudadano[3501].

De una interpretación conjunta de ambos preceptos se deduce que lo que pretende evitar la Ley es que se tomen decisiones infundadas, que puedan perjudicar a una persona basándose únicamente en tratamientos de datos dirigidos a valorar el comportamiento o aspectos de la personalidad de dicho sujeto. El objetivo consiste en evitar que se saquen conclusiones sobre el comportamiento de las personas basándose sólo en un cruce de datos, pensando, sobre todo, en ámbitos como el laboral, el de las aseguradoras o el bancario, en los que las consecuencias de las decisiones pueden ser especialmente gravosas. Se pueden tratar datos, se pueden realizar estimaciones basándose en esos datos, e incluso se pueden tomar decisiones, también perjudiciales, apoyándose en esas valoraciones. Sin embargo, no se puede hacer lo propio basándose exclusivamente en éstas[3502].

Como componente del derecho a la impugnación, la LOPD reconoce la facultad de recabar información del responsable del fichero, sobre los criterios y el programa que ha empleado para realizar la manipulación de datos de la que deriva la valoración que fundamenta la decisión que se pretende impugnar[3503]. Cuando se trata de decisiones administrativas, esta previsión deriva también de la normativa común reguladora del procedimiento administrativo, que exige que todo acto que limite los derechos subjetivos de un ciudadano sea motivado, explicando las razones

[3498] HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 248, entiende que es positivo que la LOPD no recoja, como lo hace la Directiva, europea una lista de los aspectos de la persona a evaluar "por cuanto que pudiera llegar a restringir el derecho de impugnación a las decisiones basadas exclusivamente en los tratamientos automatizados referidos únicamente a tales aspectos de la personalidad". Se entiende que la Directiva europea simplemente enumera una serie de ejemplos de lo que se puede considerar como cualidades de la persona, cosa que es positiva, por cuanto que ayuda a comprender mejor el precepto.

[3499] PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 327: reconoce la aplicabilidad directa de las excepciones de la Directiva al ejercicio de la impugnación de valoraciones. Reconoce la gran amplitud objetiva en que se puede ejercer el derecho a impugnar valoraciones; LÓPEZ DEL MORAL ECHEVERRÍA, "Impugnación de valoraciones…", cit., 2010, p. 1.132.

[3500] HERRÁN ORTIZ, *El Derecho a la Intimidad...,* cit., 2002, p. 248: la Directiva establece, en relación a la impugnación de valoraciones una lista de elementos a evaluar: trabajo…, mientras que la LOPD no. La autora considera positiva la letra de la Ley, porque así no se cierran puertas a nuevos criterios.

[3501] COLLADO GARCÍA-LAJARA, *Protección de Datos*..., cit., 2000, p. 38: "la personalidad de los interesados no puede predeterminarse, ni pública ni privadamente, valorando aptitudes o comportamientos personales, mediante el tratamiento de sus datos con relevancia jurídica, utilizando categorías generales, colectivas, etc. o estándares sociales, so pena de atentar a su honor o intimidad".

[3502] GAY FUENTES *Intimidad y Tratamiento...*, cit., 1995, pp. 83-84; MERCEDES SERRANO PÉREZ, *El Derecho Fundamental...*, cit., 2003, p. 374.

[3503] Artículo 13.3 de la LOPD.

que han llevado a adoptar dicha decisión[3504]. En general, esta facultad consiste en una prerrogativa previa, evidentemente, al ejercicio del derecho, propiamente dicho, de impugnación. Antes de que se pueda oponer a la decisión empleando los medios que ofrece el ordenamiento, será necesario que el titular de los datos conozca cómo se llegó a tomar la citada decisión[3505].

C) Cabe llamar la atención también sobre cierta divergencia que surge de la comparación entre las diferentes normas que se han citado. Cuando se refiere a los tratamientos en los que se basa la decisión que puede ser impugnada, la LOPD cita el tratamiento de datos, en términos generales[3506]. La LORTAD, fiel a su filosofía, exigía en su artículo 12 que el tratamiento de datos fuera automatizado para que la decisión pudiera ser impugnada[3507]. La Directiva europea también se refiere al tratamiento automatizado de datos[3508].

Es cierto que la informática juega un papel fundamental a la hora de entender el origen de este derecho, pues es la que plantea mayores posibilidades para cruzar y relacionar datos de carácter personal, e incluso para sacar conclusiones automáticamente de ese cruce de datos, lo que se ha venido en llamar informática decisional. Incluso se puede aceptar que en esencia este derecho tenga como fin evitar que un ordenador tome las decisiones automáticamente basándose en una serie de datos[3509]. Sin embargo, en contra de lo que ha señalado parte de la doctrina[3510], no se cree que haya que excluir de la aplicación de estos preceptos a los tratamientos de carácter manual, pues de ellos, y sin ayuda de ningún ordenador, también son deducibles, y sin mayor fundamento, valoraciones que pueden servir de soporte para la toma de decisiones perjudiciales para el titular de los datos[3511]. La Ley estatal reconoce, por lo tanto, una

[3504] Artículo 54 de la Ley 30/1992: "*Motivación.- 1. Serán motivados, con sucinta referencia de hechos y fundamentos de derecho: a) Los actos que limiten derechos subjetivos o intereses legítimos".*

[3505] HERRÁN ORTIZ, *El Derecho...*, cit., 2002, p. 249: "la obligación del responsable no puede ni debe quedar restringida a ofrecer información al interesado sobre los criterios de valoración y programas utilizados en el tratamiento y en la decisión, sino que dicha información ha de constituir un paso previo e ineludible para el responsable del fichero, de suerte que ofrezca al interesado elementos de juicio y valoración para después poder impugnar los actos o decisiones que le perjudicaban y se han basado en esas valoraciones"; GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, p. 292: el 13.3 LOPD plantea problemas prácticos: señala que cuando se impugne el titular podrá tener acceso a los criterios de valoración, etc. Pero, ¿cómo va a impugnar si antes no conoce dichos criterios? ¿No debería ser al revés (primero acceder a los criterios y luego impugnar)? Quizás el derecho de acceso sea el camino para corregir esta carencia, en atención al 12 Directiva.

[3506] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 247: en relación al derecho a impugnar valoraciones en la Directiva se emplea el concepto de "automatizado" y en la LOPD no, lo cual llama la atención.

[3507] Artículo 12 LORTAD: "*El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento cuyo único fundamento sea un tratamiento automatizado de datos de carácter personal que ofrezca una definición de sus características o personalidad".*

[3508] Artículo 15 Directiva 95/46/CE. DEL PESO NAVARRO, *Ley de Protección…*, cit., 2000. p. 52, critica el hecho de que en la LOPD no se haya incorporado el calificativo de automatizado. Señala que "aquí ha sufrido un error el legislador y no ha transpuesto fielmente la Directiva comunitaria. Ello ha sido debido quizás a ese afán de suprimir la palabra automatizado de todos los lugares".

[3509] GUICHOT, *Datos Personales...*, cit., 2005, p. 394: "la *ratio* última de la protección excedería de la protección de la intimidad para situarse en una óptica más amplia, referida a la necesaria garantía frente a la elaboración de perfiles que puedan condicionar la libertad de autodeterminación personal; a la proscripción del decisionismo automatizado".

[3510] PUENTE, "Derechos de las personas…", cit., 2008, p. 360, señala que si se incluyen los tratamientos manuales la impugnación podrá exigirse por el titular de los datos en toda manipulación.

[3511] FERNÁNDEZ SALMERÓN, *La Protección de datos…,* cit., 2003, p. 382, si bien reconoce que este derecho se vincula fundamentalmente con el tratamiento automatizado de los datos, no cierra las puertas a que se pueda ejercer sobre manipulaciones manuales.

regulación más garantista. Llama la atención, en este sentido, que el reglamento que desarrolla esta Ley retome la redacción de la Directiva, haciendo referencia al tratamiento automatizado.

En lo relativo a la forma de ejercer el derecho nada dice la normativa española, más allá de lo recogido en el RDLOPD sobre el procedimiento común para el ejercicio de los derechos de las personas[3512]. En este sentido extraña que no se haya dispuesto que el derecho a la impugnación pueda hacerse efectivo en una primera instancia ante la Agencia de Protección de Datos que corresponda, como ocurre con los derechos de acceso, oposición, rectificación o cancelación[3513]. ¿Hay que entender que el titular debe acudir a las vías ordinarias de impugnación que reconoce el ordenamiento, principalmente a Jueces y Tribunales? Se interpreta aquí que el titular cuenta con la facultad de acudir a la agencia de protección de datos correspondiente. El hecho de que el derecho a impugnar se regule tanto en la Directiva como en el RDLOPD en el apartado dirigido a la oposición da a entender que la posibilidad de requerir la tutela de la citada institución, reconocida para la oposición, sea aplicable también en este caso. Hay que tener en cuenta, además, que el derecho a la tutela de los derechos es aplicable, más allá de los casos en que se ha denegado el acceso, la cancelación, rectificación u oposición, según la Ley, a todos los casos en que hay una actuación contraria a lo dispuesto en su articulado[3514]. Lo más complicado para el titular de los datos será demostrar que la decisión que le perjudica se tomó basándose únicamente en una valoración fundamentada exclusivamente en un tratamiento de datos[3515].

La LOPD no recoge excepción alguna para este derecho. Sin embargo, como se ha visto, el RDLOPD ha traído al ámbito interno la regulación aportada por la Directiva europea y se hace eco de algunos supuestos en que queda limitado el derecho del titular de los datos a impugnar las valoraciones. Cuando una norma con rango legal así lo disponga o la valoración se haya realizado en el marco de la celebración de un contrato se podrá exceptuar este derecho. La aplicación de estas excepciones ha tenido reflejo en la práctica. La jurisprudencia estatal ha reconocido la posibilidad de limitar este derecho en supuestos en que la valoración sobre el comportamiento y personalidad de las personas titulares del derecho resulta necesaria para proteger fines de interés general[3516]. En todo caso, cuando se pretenda exceptuar este derecho, se deberá garantizar que el titular de los datos cuente con vías para defender su posición ante la valoración que se haya realizado sobre su personalidad o comportamiento. Bien sea en el ámbito

[3512] APARICIO SALOM, *Estudio sobre la Ley…,* cit., 2009, p. 248, critica esta circunstancia debido a que impide que el derecho pueda ser reconocido en la práctica.
[3513] GUICHOT, *Datos Personales…,* cit., 2005, p. 396.
[3514] Artículo 18.1 LOPD.
[3515] CARDONA RUBERT, *Informática y Contrato…*, cit., 1999, p. 136; PUYOL MONTERO, "Los derechos de acceso…", cit., 2008, p. 329: habla de la dificultad de probar que las decisiones que se adoptaron se hicieron únicamente basándose en las valoraciones; GARRIGA DOMÍNGUEZ, *Tratamiento de Datos…,* cit., 2009, p. 130; LÓPEZ DEL MORAL ECHEVERRÍA, "Impugnación de valoraciones…", cit., 2010, p. 1.135.
[3516] SAP de Madrid 21 de marzo de 2006, FJ 3: una persona presa impugna la valoración que se hace de su condición como Interno de Especial Seguimiento, en la medida en que esta inclusión conlleva una serie de efectos jurídicos, como la aplicación de un régimen penitenciario más severo. Apunta que esta decisión se fundamenta exclusivamente en un tratamiento de datos destinado a evaluar su personalidad. Se señala que la decisión se basa en el tratamiento de datos sobre la condición penal, procesal y penitenciaria de las personas presas. SAP de Ciudad Real 7 de marzo de 2005, FJ 2: en una sentencia concerniente a la misma materia, señala que las valoraciones que se realizan tras recoger los datos de las personas presas y las decisiones que se toman en base a dichas valoraciones, tienen como fin garantizar la adecuada convivencia y la seguridad en los centros penitenciarios. No se trata de valoraciones arbitrarias, sino fundadas en datos objetivos sobre las personas presas.

de un contrato o bien porque así lo ha autorizado una ley, lo fundamental en cuanto a estas excepciones será que el titular de los datos pueda plantear en todo momento su punto de vista y defender su posición ante cualquier decisión que pueda perjudicarle.

En un principio podría decirse que la aplicabilidad de este derecho en el ámbito sanitario es amplia, en la medida en que se ha dicho que en este sector es común o constante la realización de valoraciones. No obstante, esta posible aplicabilidad se reduce si se hace un análisis algo más profundo. En el ámbito sanitario las valoraciones basadas en datos relativos a los pacientes son continuas: se interpretan los datos sanitarios y se extraen estimaciones sobre el comportamiento del cuerpo y de la mente del paciente, y partiendo de esas valoraciones se toman decisiones que afectan a este último. Sin embargo, no parece que estas valoraciones sean las referidas en la LOPD cuando regula el derecho de impugnación. En la gran mayoría de los casos, por no decir siempre, en el ámbito sanitario las decisiones suelen estar bien fundamentadas y contrastadas con pruebas de diferente entidad. Además, el fin de estas decisiones no es, ni mucho menos, perjudicial para el paciente, pues se trata de asistir a la persona de la mejor forma posible de acuerdo con la *lex artis*. En el caso que aquí se analiza las valoraciones que se extraen de los datos no se dirigen a adoptar decisiones perjudiciales para los titulares de los datos, sino que son opiniones de profesionales sanitarios que tienen como objetivo la protección de la persona. Hay que tener en cuenta además, que la aplicabilidad de este derecho con todo su rigor afectaría al ejercicio de la actividad sanitaria. Ésta se basa en la realización de valoraciones. Si los profesionales de la sanidad no pudieran llevar a cabo estas apreciaciones, los diagnósticos serían imposibles de llevar a cabo, por lo que su actividad sería dificultosa. En conclusión, no es fácil encajar el derecho a la impugnación de valoraciones en el ámbito sanitario.

VI. DERECHO A LA INDEMNIZACIÓN.

VI.1. El significado del derecho a la indemnización y breve referencia a las distintas vías para reclamarla.

Junto a los derechos analizados hasta ahora la LOPD reconoce en un apartado específico, al contrario de lo que hacía la normativa estatal anterior[3517], un derecho de gran relevancia práctica como es el derecho a la indemnización. El sentido de la inclusión de este derecho en la vigente Ley orgánica de protección de datos es evidente. Cuando la acción de un responsable o encargado de tratamiento incumple lo dispuesto en la LOPD dicha actuación será objeto de sanciones, que se prevén también en la misma Ley y que, hay que decirlo, son en este ámbito especialmente duras o gravosas. Sin embargo, más allá del hecho de que la AEPD o los tribunales puedan imponer sanciones a quienes incumplen el contenido de las normas, las actuaciones de responsables y encargados pueden causar daños a los titulares de los datos que den derecho a una indemnización. Piénsese en el caso en que una historia clínica, que refleja

[3517] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 258: señala la importancia de que la LOPD haya entrado a regular el derecho a la indemnización, que no venía en la LORTAD. Importante porque en la actualidad son muchas las fórmulas para causar daños con el tratamiento de datos; GUICHOT, *Datos personales…,* cit., 2005, p. 410: el derecho de indemnización existiría incluso sin que se mencionara en la normativa protección de datos pues así lo exige el ordenamiento civil y administrativo ante la causación de un daño.

que un sujeto ha sido infectado por el VIH, ha sido perdida por un centro sanitario y la documentación se recoge por terceros que acaban por tomar decisiones perjudiciales para dicha persona, como puede ser su despido del trabajo[3518]. Partiendo del clásico principio de que quien causa un daño tiene que repararlo, las normas han admitido expresamente que en estos casos es posible acudir a las vías ordinarias para exigir responsabilidad al responsable o encargado del tratamiento y obtener una indemnización, sin necesidad de acudir previamente a la agencia de protección de datos correspondiente[3519].

La regulación que la LOPD lleva a cabo de este derecho trae causa de lo dispuesto en la Directiva europea[3520]. Esta regulación es especialmente parca y no entra a concretar con suficiente rigor los requisitos que han de cumplirse para solicitar la indemnización. La Ley reconoce simplemente el derecho del titular de los datos a ser indemnizado en los casos en que sufra algún daño o lesión en sus bienes o derechos debido al incumplimiento de lo dispuesto en la LOPD por el responsable o encargado del tratamiento[3521], y determina que la exigencia de la indemnización se realizará dependiendo de si se trata de ficheros públicos o privados en base a la normativa reguladora de la responsabilidad patrimonial de la Administración o en la jurisdicción ordinaria[3522]. Esta regulación no ha encontrado desarrollo en el RDLOPD. Por su parte, la jurisprudencia ha aplicado en muchas ocasiones el artículo 19 LOPD, la mayoría de veces refiriéndose a un supuesto concreto como es el caso en que el responsable mantiene datos erróneos sobre la morosidad de una persona[3523], pero no ha desgranado cuáles son las características del derecho a la indemnización reconocido en la Ley. Tampoco la doctrina se ha prodigado en analizar el contenido de este derecho.

El análisis de la regulación que realiza la LOPD podría dividirse en dos apartados. El primero, relativo a un aspecto formal y dedicado al procedimiento que se ha de seguir para la reclamación de la indemnización, y el segundo, que será estudiado en el apartado siguiente, destinado a analizar las características del incumplimiento del responsable o encargado al que se refiere el artículo 19 de la Ley y que da lugar al derecho a la indemnización.

En lo que toca al primero la LOPD realiza una remisión a las normas que regulan la responsabilidad patrimonial de la Administración y la jurisdicción ordinaria. Evidentemente,

[3518] STEDH 17 de julio de 2008, I. v. Finlandia, FFJJ 53 y siguientes, en los que se admite el derecho de indemnización a una persona seropositiva, por daños patrimoniales y morales causados por accesos indebidos a su historia clínica por personas que no estaban implicadas en su tratamiento sanitario.

[3519] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., p. 257.

[3520] Artículo 23 Directiva 95/46/CE: "*1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño*".

[3521] Artículo 19.1 LOPD.

[3522] Artículo 19.2 y 19.3 LOPD.

[3523] SAP de Islas Baleares 13 de octubre de 1998; SAN 29 de abril de 2004, FJ 4: señala que el mero mantener de unos datos más del tiempo debido sin haberlos cancelado da derecho a indemnización. Sin embargo, esta vulneración del derecho a la protección de datos se reconoce como acarreadora de derecho a la indemnización en la medida en que queda probado que dicha circunstancia le causó daños al titular: la empresa que conservó los datos del trabajador más de lo debido no los puso en conocimiento del propio trabajador titular de los datos impidiendo que éste último tuviera todos los medios posibles de defensa en un procedimiento laboral paralelo.

resulta imposible afanarse en este momento en describir al detalle qué requisitos son necesarios y qué procedimiento se ha de seguir, para que el titular de los datos pueda exigir una indemnización bien a una Administración pública o bien a persona privada, pues reclamaría una labor que excede de las pretensiones de este trabajo. Bastará con una breve referencia a las distintas posibilidades que el afectado tiene para exigir la indemnización.

La reclamación se realizará dependiendo de si el responsable es una Administración o una persona privada. A) En relación al primer caso, la indemnización podrá exigirse empleando el procedimiento común para solicitar la responsabilidad patrimonial de la Administración. Primero se hará ante la Administración responsable[3524] y posteriormente ante los Jueces y Tribunales de la jurisdicción contencioso-administrativa. Ante los tribunales la indemnización podrá solicitarse a través de la vía ordinaria o empleando el procedimiento especial para la protección de los derechos fundamentales previsto por la LJCA[3525].

Por esta vía la indemnización podrá reclamarse basándose exclusivamente en el artículo 19.1 LOPD, que se analizará en el apartado siguiente, si la actividad del responsable o encargado del tratamiento encaja en el comportamiento descrito en ese precepto. Sin embargo, esta reclamación también podrá realizarse en atención a las reglas comunes que describen las actuaciones que dan lugar a la responsabilidad patrimonial de la Administración. Según la LPAC la Administración responde por los daños causados por el funcionamiento normal o anormal de los servicios públicos, siempre que el daño sea efectivo, individualizado y económicamente evaluable, y el afectado no tenga el deber jurídico de soportar la lesión o que no haya un caso de fuerza mayor que lo justifique[3526]. En caso de que se cause un daño al derecho a la autodeterminación informativa que cumpla con las características citadas, la reclamación de la indemnización se realizará empleando el procedimiento común para solicitar la responsabilidad patrimonial de la Administración. El que la indemnización se exija frente a una Administración puede constituir una ventaja si se atiende a las especiales características de la responsabilidad patrimonial de la Administración, sobradamente analizadas por la doctrina[3527]. Partiendo de que responde tanto de su funcionamiento anormal como normal[3528], la responsabilidad de la Administración ha sido calificada como objetiva, interpretando que la Administración ha de responder incluso cuando el daño se ha causado sin que haya existido negligencia en la actuación de las personas a su servicio[3529]. La Administración respondería en todo caso, siempre que se causara un daño. La aplicación de este criterio en el ámbito sanitario plantea, sin embargo, grandes problemas prácticos teniendo en cuenta que la obligación de los profesionales es de poner todos los medios a su alcance para asistir a las personas y no de resultados, y que

[3524] Artículos 139 y siguientes LPAC; RD 429/1993, 26 de marzo, por el que se aprueba el Reglamento en Materia de Responsabilidad Patrimonial de las Administraciones Públicas.
[3525] Artículo 114 LJCA.
[3526] Artículo 139 y 141.1 LPAC.
[3527] SÁNCHEZ MORÓN, *Derecho Administrativo…*, cit., 2009, p. 911; MEDINA ALCOZ, "La responsabilidad patrimonial…", cit., 2009; QUINTANA LÓPEZ (Dir.) y CASARES MARCOS (Coord.), *La Responsabilidad Patrimonial…*, cit., 2009; PULIDO QUECEDO, *Responsabilidad Patrimonial…*, cit., 2010.
[3528] Artículo 139.1 LPAC.
[3529] GONZÁLEZ PÉREZ, *Responsabilidad Patrimonial…*, cit., 1996, p. 138; DE AHUMADA RAMOS, *La Responsabilidad Patrimonial…*, cit., 2004, p. 55; MENÉNDEZ SEBASTIÁN, "Principios de la responsabilidad…", cit., 2009, p. 45; PULIDO QUECEDO, *Responsabilidad Patrimonial…*, cit., 2010, pp. 162-163.

el riesgo de causar daños es inherente a la actividad sanitaria[3530]. A pesar de ello, frente a posturas que han tratado de flexibilizar el criterio de la responsabilidad objetiva[3531], ésta se ha defendido en algún caso también para las administraciones sanitarias[3532]. La asunción de esta posición podría llevar a ampliar los supuestos en que se puede solicitar una indemnización, con respecto a los casos en que se reclama responsabilidad civil.

B) Cuando se trata de una persona privada la indemnización podrá solicitarse a través del procedimiento penal o civil[3533]. En el primer caso, cuando la actuación sancionable del responsable o encargado del tratamiento pueda encuadrarse en alguno de los tipos recogidos en el CP, normalmente los descritos en el artículo 197 y siguientes referentes a los delitos contra la intimidad, la indemnización se solicitará, conforme viene establecido en el propio CP[3534], o bien en la vía penal, siguiendo los criterios marcados en la norma penal, o en la vía civil, en cuyo caso se atenderá a los criterios establecidos en el CC. En el segundo caso, si la acción del responsable no constituye una infracción penal, la indemnización se solicitará en la vía civil. La reclamación de indemnización en esta vía se realizará, dependiendo de lo solicitado y de la cuantía de la indemnización exigida, siguiendo el procedimiento correspondiente al juicio ordinario o al juicio verbal[3535].

Al igual que sucedía en el ámbito de la Administración, la reclamación podrá basarse exclusivamente en el artículo 19 LOPD o en las reglas marcadas por el CC para el nacimiento de la responsabilidad civil. La reclamación de la indemnización en este último caso deberá llevarse a cabo atendiendo a distintos criterios, dependiendo de si hay una relación contractual entre el médico o centro privado y el paciente, en cuyo caso habrá de estarse a lo dispuesto en el artículo 1.101 CC regulador de la responsabilidad contractual, o si no la hay, supuesto en que deberán tenerse en cuenta los artículos 1.902 CC y siguientes reguladores de la responsabilidad extracontractual. A la hora de determinar si existe o no la responsabilidad civil que da lugar al derecho de indemnización habrá de tenerse en cuenta que aquí no existe la responsabilidad objetiva que se ha descrito más arriba, sino que se trata de una responsabilidad subjetiva de manera que es necesario que el responsable cause el daño de forma voluntaria o mediando culpa o negligencia[3536]. En este caso, el funcionamiento normal del centro sanitario no conllevaría responsabilidad.

La exigencia de responsabilidad a los centros puede realizarse también atendiendo a otras normas. Primero, podría basarse en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias[3537]. En lo que afecta a los servicios

[3530] CUETO PÉREZ, *Responsabilidad de la Administración…*, cit., 1997, p. 229; RODRÍGUEZ LÓPEZ, *Nuevas Formas de Gestión…*, cit., 2004, pp. 101-106; BELLO JANEIRO, *Responsabilidad Civil…*, cit., 2009, p. 125.
[3531] PANTALEÓN, *Responsabilidad médica…*, cit., 1995, p. 73-79; MIR PUIGPELAT, *La Responsabilidad Patrimonial…*, cit., 2000, pp. 40-41; BELLO JANEIRO, *Responsabilidad Civil…*, cit., 2009, p. 204.
[3532] CUETO PÉREZ, *Responsabilidad de la Administración…*, cit., 1997, pp. 230-233.
[3533] RUIZ CARRILLO, *La Protección de los Datos…,* cit., 2001, pp. 109-110.
[3534] Artículos 109 y siguientes CP.
[3535] Artículo 249.1.2, 249.2 y 250 LEC.
[3536] BELLO JANEIRO, *Responsabilidad Civil…*, cit., 2009, pp. 47-48.
[3537] Artículo 128 RDL 1/2007, 16 de noviembre, por el que se aprueba le Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias.

sanitarios dispone esta norma que se responderá "*(…) de los daños originados en el correcto uso de los servicios, cuado por su propia naturaleza, o por estar así reglamentariamente establecido, incluyan necesariamente la garantía de niveles determinados de eficacia o seguridad, en condiciones objetivas de determinación, y supongan controles técnicos, profesionales o sistemáticos de calidad, hasta llegar en debidas condiciones al consumidor y usuario*"[3538]. Tanto la jurisprudencia como la doctrina han afirmado que este precepto es aplicable a los servicios que prestan los centros sanitarios, cuando menos en lo que afecta a la actividad administrativa o de gestión organizativa[3539], en la que se podría englobar gran parte de la acción de manipulación de datos en este ámbito. La referencia que en el citado precepto se realiza a "los daños originados en el correcto uso de los servicios" se ha entendido en algún caso como una fórmula que incorpora en este ámbito la forma objetiva de responsabilidad, como sucedía en la responsabilidad patrimonial de la Administración[3540].

Segundo, la responsabilidad podría fundarse en la LO 1/1982, 5 de mayo, de protección civil del Derecho al Honor, Intimidad Personal y Familiar y a la Propia Imagen. No es improbable que la actuación de un responsable del fichero o un encargado de tratamiento afecte a alguno de los indicados derechos, principalmente al derecho de intimidad. Cuando esto ocurre, la indemnización puede reclamarse en atención a lo que dispone la señalada Ley orgánica en su artículo 9.

Más allá de las distintas vías que se pueden emplear para reclamar una indemnización por vulneración del derecho a la autodeterminación informativa, lo que realmente interesa a efectos prácticos es determinar cuándo se entiende que hay una lesión o daño que pueda dar lugar a ese derecho en base al artículo 19 LOPD. El mayor problema a la hora de exigir responsabilidades surge, en lo que afecta al ámbito de la protección de datos sanitarios, al determinar si se ha producido un daño[3541].

VI.2. La reclamación de indemnización en atención al artículo 19.1 LOPD. La necesidad de probar que ha habido un daño.

La LOPD señala que cuando un incumplimiento de la Ley produzca un daño o lesión surgirá el derecho a reclamar la indemnización. Esta expresión que en un principio no parece plantear problemas interpretativos de relevancia ha de ser analizada con cierta procura. Sobre esta expresión deben hacerse principalmente dos consideraciones.

Primero, hay que tener en cuenta que la letra de la Ley exige que el daño se produzca por un incumplimiento del responsable o encargado del tratamiento. La referencia al hecho de que se haya de dar un "incumplimiento" lleva a concluir que debe haber un comportamiento incorrecto de

[3538] Artículo 148 RDL 1/2007, 16 de noviembre, por el que se aprueba le Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras Leyes Complementarias.
[3539] STS 23 de octubre de 2008, FJ 4. BELLO JANEIRO, *Responsabilidad Civil…*, cit., 2009, p. 90.
[3540] BELLO JANEIRO, *Responsabilidad Civil…*, cit., 2009, p. 87.
[3541] PUYOL MONTERO, "Derecho a indemnización…", cit., 2010, p. 1.263, realiza un interesante análisis al respecto.

los señalados sujetos para poder argumentar el artículo 19 LOPD[3542]. De esta manera, la indemnización en atención a este precepto no podrá derivar de un comportamiento correcto o normal, que cumpla con los requisitos exigidos por la normativa de protección de datos.

Segundo, y este es el punto más polémico, deberá existir un daño o lesión que justifique la reclamación de la indemnización. Independientemente de si la exigencia se realiza a una Administración o a un centro privado lo más complejo será concretar si se ha producido un daño susceptible de ser indemnizado.

El concepto de daño ha sido analizado en numerosas ocasiones, sobre todo desde la doctrina iuspublicista. Más allá de la lógica exigencia de que la lesión sea efectiva, evaluable económicamente e individualizable, la LPAC requiere para que exista derecho a la indemnización que el lesionado no tenga obligación de soportar la lesión[3543]. En términos genéricos, por lo tanto, en lo que toca a la lesión deberán tenerse en cuenta dos aspectos.

A) Trasladando lo indicado al ámbito que aquí se estudia, si la actuación del responsable o encargado conlleva una lesión pero hay un motivo que justifica su acción e impone al afectado el deber de soportarla, no podrá solicitarse una indemnización. La necesidad de determinar cuándo existe ese deber de soportar el daño parece obvia. La LOPD no dice nada sobre las causas de exclusión de responsabilidad por el tratamiento de datos. Sin embargo, la Directiva europea de protección de datos se refiere a modo de ejemplo a la fuerza mayor y a la responsabilidad del propio titular de los datos en la causación del daño[3544]. Partiendo de esta regulación y haciendo una interpretación sistemática de las normas de protección de datos parece que no hay problemas para admitir que no habrá derecho a la indemnización si el daño se ha producido con el consentimiento del titular de los datos, en atención a las causas que exceptúan el derecho al consentimiento previstas en la LOPD, mediando la responsabilidad del propio titular de los datos o por la existencia de casos de fuerza mayor y, cuando se trata de la responsabilidad civil, casos fortuitos[3545].

B) Más allá de que tercie o no el deber de soportar el daño, para que exista indemnización deberá analizarse si efectivamente la lesión existe. Cuando a raíz de la actuación de un responsable se produzcan perjuicios económicos no se presentan mayores dificultades. Las dificultades surgen en relación a los daños morales, por el hecho de que los titulares de los datos pudieran alegar este tipo de lesiones siempre que una actuación del responsable del fichero vulnere la LOPD[3546]. A este respecto parece que se ha asumido una posición significativamente amplia o expansiva.

[3542] BUISÁN GARCÍA, "Derechos de las personas…", cit., 2008, p. 397; PUYOL MONTERO, "Derecho a indemnización…", cit., 2010, p. 1.267.
[3543] MEDINA ALCOZ, "Responsabilidad patrimonial…", cit., 2009, pp. 75-76; PULIDO QUECEDO, *Responsabilidad Patrimonial…*, cit., 2010, p. 180.
[3544] Considerando 55 Directiva 95/46/CE.
[3545] DE AHUMADA RAMOS, *La Responsabilidad Patrimonial…*, cit., 2004, p. 221, se ha entendido que el caso fortuito no exime a la Administración de la responsabilidad.
[3546] EGUSQUIZA BALMASEDA, *Protección de Datos…,* cit., 2009, p. 183, hace también referencia a este hecho.

El ordenamiento parece apostar por un concepto amplio de responsabilidad, dando pie a que se pueda entender que toda vulneración de la LOPD que afecte a los datos de alguien puede otorgar derecho a indemnización. En esta línea se ha llegado a reconocer que la previsión de la Ley puede constituir base para asumir una responsabilidad objetiva[3547]. Siempre que haya un incumplimiento y un daño parece que habrá derecho a la indemnización, independientemente de si existe un elemento de culpabilidad o no[3548]. No se va a ahondar en este momento en la consideración de esta responsabilidad como objetiva o subjetiva; sin embargo, interesa saber que se ha ido apostando por un concepto amplio de responsabilidad por cuanto esta visión se ha venido reforzando también debido a la idea de la existencia de lo que se podría llamar una "presunción de daño".

En muchas ocasiones ha parecido que cuando se da un incumplimiento de la Ley se presume que se ha producido un daño o lesión al titular de los datos. Parte de la doctrina ha apoyado esta consideración[3549], que podría fundamentarse también en previsiones normativas dirigidas a proteger los derechos al honor, la intimidad y la imagen, que, como apunta también la jurisprudencia, parecen abogar por esta presunción[3550]. En la misma línea, refiriéndose ahora al ámbito de la protección de datos, la jurisprudencia ha adoptado en alguna ocasión una posición muy flexible, reconociendo por ejemplo que la inclusión errónea de una persona en un fichero de morosos genera *per se*, independientemente de que un tercero haya accedido o no al fichero, daños morales[3551].

[3547] GRIMALT SERVERA, *La responsabilidad civil…,* cit., 1999, p. 149; PUYOL MONTERO, "Derecho a indemnización…", cit., 2010, p. 1.282.

[3548] GRIMALT SERVERA, *La responsabilidad civil…,* cit., 1999, pp. 153-154; VALERO TORRIJOS, *Comentarios a la Ley…,* cit., 2001, pp. 222-223; GUICHOT, *Datos personales…,* cit., 2005, pp. 410-414; GUERRERO PICÓ, *El impacto de Internet…,* cit., 2006, p. 309.

[3549] HERRÁN ORTIZ, *El Derecho a la Intimidad…,* cit., 2002, p. 260, parece apoyar esta posición.

[3550] Artículo 9.3 LO 1/1982: "*La existencia de perjuicio se presumirá siempre que se acredite la intromisión ilegítima. La indemnización se extenderá al daño moral que se valorará atendiendo a las circunstancias del caso ya la gravedad de la lesión efectivamente producida, para lo que se tendrá en cuenta en su caso, la difusión o audiencia del medio a través del que se haya producido*". En relación a este punto SAP de Barcelona 3 de mayo de 2000, FJ 4: "establece una presunción legal de producción de perjuicio siempre que se acredite al intromisión ilegítima, lo que supone que de tal intromisión debe seguirse una indemnización, comprensiva del daño moral y valorable en atención a las circunstancias del caso, a la gravedad de la lesión efectivamente producida en relación con la difusión del hecho divulgado". GRIMALT SERVERA, *La responsabilidad civil…,* cit., 1999, p. 140, considera aplicable esta previsión en el ámbito de la protección de datos, afirmando que "siempre que haya existido un tratamiento ilegítimo se podrá presumir que ha existido un daño"; MINGORANCE GOSÁLVEZ, "La reparación del daño…", cit., 2010, p. 2.634.

[3551] STS 24 de abril de 2009, FJ 2: "esta sala, en pleno, ha mantenido la posición de entender que la inclusión fallando a la veracidad, por una entidad, en un registro de solvencia patrimonial –los llamados "registros de morosos"- implica un atentado al derecho del honor del interesado que ha aparecido en tal registro, erróneamente (…)". "Y es intrascendente el que el registro haya sido o no consultado por terceras personas, ya que basta la posibilidad de conocimiento por un público, sea o no restringido y esta falsa morosidad haya salido de la esfera interna del conocimiento de los supuestos acreedor y deudor, para pasar a ser de una proyección pública". Sentencia Juzgado de Primera Instancia de Valencia 5 de octubre de 2005, FJ 3: en el caso concreto, se señala que la inclusión errónea de una persona en ficheros de morosos genera "una situación de zozobra o ansiedad" "además de molestias y pérdida de tiempo en arreglar lo que, solo por causa imputable a Uni2, se desarregló". SAN 14 septiembre 2001, FJ 3, en la que se da a entender que el hecho de que el responsable del fichero no haga efectivo el derecho de cancelación ejercido por el titular de los datos constituye en sí mismo un daño, en la medida en que lesiona el derecho de dicho titular a controlar lo que sucede con sus datos de carácter personal. No parece exigir nada más. De esta manera se decanta por una visión especialmente amplia, pues si toda afección al derecho a la autodeterminación informativa constituye un daño, se puede llegar a entender que existe indemnización cada vez que se incumple la LOPD: "De este modo, no cabe razonar como lo hace el recurrente, que no existe daño, porque no hay agresión o lesión de la esfera privada o intimidad

Esta interpretación podría llevar a situaciones difíciles de asimilar. Imagínese el caso en que un responsable o encargado de fichero incumple la obligación de adoptar determinadas medidas de seguridad, sin que esta situación haya llevado a la pérdida o alteración de datos. Esta actuación constituiría una circunstancia merecedora de sanción, tal y como señala la LOPD[3552]. Pero además, siguiendo los criterios que se acaban de plantear, se llegaría a pensar que el titular de los datos tiene ante esta circunstancia el derecho a una indemnización.

Atendiendo a una interpretación más estricta que la arriba indicada, y haciendo referencia al caso señalado sobre la inclusión errónea de datos en un fichero de morosos, no resulta fácil justificar en este supuesto la existencia de un daño efectivo en la medida en que ningún tercero ha accedido a dichos datos, ni los ha manipulado. Podría argumentarse que al tratarse de datos erróneos se causaba al titular de los mismos una situación de inseguridad y desasosiego generadora de un daño moral merecedor de reparación. Más allá de estos supuestos daños morales constituye tarea difícil imaginar otra lesión. Incluso en los casos en que se haya asumido la existencia de daños morales, debería plantearse si el titular de los datos tiene en estos supuestos, tan dudosos, derecho a recibir una compensación económica. Hay que tener en cuenta que tanto el TC como el TEDH han señalado en diferentes decisiones que la reparación de la lesión puede darse en ocasiones a través de la mera declaración de que la lesión se ha producido y con el reconocimiento del derecho[3553].

La ecuación que llevaría a admitir que cualquier incumplimiento de la Ley vulnera el derecho a la autodeterminación informativa del titular de los datos y que, por lo tanto, esa vulneración constituye una lesión susceptible de indemnización ha de ser rechazada. Evidentemente, todo incumplimiento de la Ley supone una actuación sancionable por la AEPD primero y, en su caso, por los Jueces y Tribunales. Sin embargo, no toda vulneración de la Ley constituye una lesión o daño que conlleve aparejado derecho a indemnización[3554]. Frente a la posición amplia señalada, la propia jurisprudencia ha realizado ciertos matices para no caer en situaciones absurdas, exigiendo en cada caso que el daño haya de probarse[3555]. Ante la pretensión, por ejemplo, de

---

personal del individuo. Pues tal razonamiento ignora la existencia del contenido positivo del derecho. En efecto, la conducta de la entidad, que pese a certificar la cancelación, no cancela y continúa utilizando el dato, supone una agresión directa y por ende una clara lesión al derecho del afectado de que sus datos no sean utilizados. El recurrente, con habilidad centra la posibilidad de lesión en el aspecto negativo del derecho; pero olvida toda referencia al aspecto positivo o poder de control sobre los mismos. Y ciertamente, es difícil imaginar lesión mayor que el mantenimiento y uso del dato, pese a la procedencia de la cancelación".

[3552] Artículo 44.3 LOPD: "*Son infracciones graves: h) Mantenerlos ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen*".

[3553] STC 29 de noviembre de 2004, FJ 5; STDEH 20 diciembre 2005, Wisse v. Francia, FJ 38: en relación a la indemnización de los daños morales causados por la grabación y posterior uso por los poderes públicos de unas conversaciones mantenidas por un sujeto, "El Tribunal estima que la constatación de la violación señalada constituiría una indemnización suficiente para compensar el daño alegado".

[3554] SSAN 8 de marzo de 2006, FJ 4; 1 de octubre de 2008, FJ 6.

[3555] SAN 12 de enero de 2001, FJ 2: se solicita responsabilidad patrimonial de la Administración por no haber cancelado datos sobre antecedentes policiales y por haber filtrado esta información a determinados sujetos que han causado al interesado perjuicios en forma de no contratación en determinados sectores, pérdida de amistades… Señala la AN que no queda probado que dichos daños se hubieran producido, por lo que no cabe indemnización alguna. SAN 31 de marzo de 2004, FJ 5: el titular de los datos llega a alegar la pérdida de confianza en las Administraciones Públicas como fuente de derecho a indemnización por daños morales. Señala la AN que esta pérdida de confianza no

reclamar indemnización alegando el sufrimiento que ha causado el hecho de que el responsable del fichero no haya contestado a la solicitud de acceso llevada a cabo por el titular de los datos, los tribunales han señalado que es necesario que se demuestre que el daño es real y efectivo[3556]. También se ha requerido por los tribunales que la causa que genera el daño sea en todo caso imputable al responsable o encargado del fichero[3557]. El daño moral ha sido definido por la jurisprudencia como el sufrimiento, tristeza, desazón o inquietud provocada por quien causa la lesión[3558]. Sin embargo, se exige que este daño pueda objetivarse por la exteriorización de datos y circunstancias concretas, que son las causantes de la sensación de zozobra, desasosiego, angustia o ansiedad[3559]. La existencia de una lesión o daño ha de probarse, por lo tanto, en todo caso. A la hora de valorar el daño moral pueden ser de utilidad los criterios marcados por la LO de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, que dispone que este daño se valorará atendiendo a las circunstancias de cada caso y a la gravedad de la lesión, teniendo que tener en cuenta, en su caso, la difusión o audiencia del medio a través del que se haya producido[3560].

Durante este trabajo se han visto casos planteados en la realidad, vinculados a la cuestión sanitaria, que generan interrogantes como la que ahora se analiza. Se ha citado el supuesto en que datos sanitarios de una persona, que simplemente reflejan revisiones ordinarias, se cuelgan durante un plazo de tiempo, por un descuido, en la red sin que se demuestre que tercero alguno haya accedido a dicha información y sin que el titular tuviera conocimiento de tal circunstancia[3561]. Se entiende aquí que no es tarea sencilla argumentar que se haya causado en este caso daño alguno. Que la acción es sancionable por la Administración no plantea duda alguna. Sin embargo, que esa acción causa un daño o lesión en el titular de los datos es más que dudoso. Por un lado porque ningún tercero ha accedido a dicha información. Y por otro, porque el contenido de la información difícilmente pudiera ser empleado como instrumento para causar

puede considerarse un concepto indemnizable, teniendo en cuenta que a través de la AEPD se han reparado las actuaciones defectuosas sobre los datos del titular y se asegura que no se volverán a suceder.

[3556] SAN 18 de enero de 2006 FJ 4: señala la AN que "Como ha señalado el Tribunal Supremo (ST 15 de julio de 2002 , entre otras) para que el perjuicio pueda ser indemnizable, los daños han de ser reales y efectivos y ha de acreditarse su existencia, lo que el recurrente no ha realizado, pues no se ha probado la existencia de gasto alguno nacido de desembolsos efectuados por la misma en relación con los escritos que ha presentado ante los distintos organismos y el procedimiento seguidos para lograr el acceso a sus datos personales, no habiendo aportado documento alguno que los justifique". "Tampoco ha resultado acreditado el daño moral invocado por el actor, dado que los procedimientos instados ante la Agencia de Protección de Datos concluyeron mediante resoluciones favorables a las pretensiones del recurrente, logrando el acceso a la totalidad de sus datos personales obrantes en el INEM y la posibilidad de rectificar los mismos, viendo así restituidos plenamente sus derechos, mediante los mecanismos legales previstos para reparar esa actuación defectuosa y evitar que en el futuro pueda volver a repetirse".

[3557] SAP de Zaragoza 30 de enero de 2009, FJ 3: para la aplicación del artículo 19 LOPD "el demandante ha de acreditar no sólo la existencia de daños o lesiones en sus bienes o derechos, sino además que los mismos derivan causalmente de la vulneración del deber de guardar secreto de los datos personales". STS 20 de abril de 2007, FJ 5: en relación al consentimiento informado en el ámbito sanitario, dirigido a la asistencia sanitaria, se señala que la falta de información por parte de la Administración sanitaria, al igual que el resto de actuaciones, para que generen derecho a ser indemnizado, es necesario que causen un daño derivado de dichos actos.

[3558] STS 22 de febrero de 2001 FJ 6. PUYOL MONTERO, "Derecho a indemnización…", cit., 2010, p. 1.277.

[3559] STS 7 de marzo de 2005 FJ 4.

[3560] Artículo 9.3 LO 1/1982, 5 de mayo de 1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen.

[3561] SAP Bizkaia 10 de noviembre de 2010.

daño alguno a dicha persona, por lo que la sensación de zozobra que pudiera justificar un daño moral es difícilmente argumentable.

En conclusión, se entiende que el ejercicio del derecho a la indemnización ha de llevarse a cabo en todo caso en base a corolarios bien definidos en que se demuestre la existencia de daños efectivos y que dichos daños han sido causados debido a una actuación imputable al responsable o encargado del fichero, sea dolosa o culposa.

Los incumplimientos de la LOPD en el ámbito sanitario pueden ser múltiples. Desde fallos en la configuración del sistema sanitario, fundamentalmente con la no adopción de las medidas de seguridad oportunas, hasta incumplimientos de carácter más sustantivo, como puede ser el no cancelar datos que han dejado de ser necesarios para cumplir las finalidades que justificaron su recogida. Como se ha dicho, el ejercicio del derecho a una indemnización exige que esos incumplimientos generen un daño al titular de los datos. Deberá demostrarse que las lesiones son reales y efectivas y que se deben a una actuación imputable al responsable.

RECAPITULACIÓN.

Resulta comúnmente asumido que las nuevas Tecnologías de la Información y la Comunicación están transformando la forma de relacionarse en los diferentes ámbitos de la vida: económico, social, cultural, político, administrativo, etc. El empleo cada vez más generalizado de estas nuevas herramientas, sobre todo de las aplicaciones derivadas de Internet, está llevando a la consolidación definitiva de la Sociedad de la Información, que se define por la especial relevancia que la información adquiere y la capacidad de sus miembros para manipularla. La información ha constituido siempre un elemento imprescindible para la organización, funcionamiento y desarrollo de las sociedades, sin embargo, en la actualidad su relevancia se ha multiplicado. Es indudable que el volumen de datos que se manejan por todo tipo de agentes, públicos y privados, es mayor que en tiempos pasados, y que las nuevas tecnologías permiten realizar más operaciones, de forma más rápida y con un alcance global. La célebre frase "información es poder" despliega hoy día todo su sentido.

La incorporación de las TIC se ha producido en todos los sectores. La Administración sanitaria no ha sido, evidentemente, ajena a este fenómeno. En este ámbito la integración de las nuevas tecnologías se está llevando a cabo poco a poco, de la mano de herramientas como la historia de salud electrónica, la tarjeta sanitaria inteligente o la receta electrónica. Prueba de ello es la cada vez más frecuente aprobación de normas que incorporan estos instrumentos en la realidad sanitaria, caso del RD 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de disposición, que integra definitivamente la receta electrónica en el Sistema Nacional de Salud, o el Decreto 29/2009, de 5 de febrero, por el que se regula el uso y acceso a la historia clínica electrónica en Galicia. En definitiva, la forma de prestar los distintos servicios sanitarios está cambiando y se está consolidando la telemedicina, entendida en sentido amplio, como una nueva forma de proteger la salud de las personas en la que las TIC juegan un papel fundamental.

Cuando se hace referencia a la telemedicina no se está hablando únicamente de un cambio en la forma de actuar de los sistemas sanitarios, sino que supone una alteración en la esencia misma de la realización de las actividades sanitarias. La incorporación de las nuevas tecnologías en este campo puede y debe conllevar, sobre todo, una evolución en la relación entre el paciente o usuario y los profesionales de la sanidad o la Administración sanitaria, que suponga una mayor participación e implicación de los primeros en los procesos que les afectan y la posibilidad de llevar a cabo nuevas operaciones como la asistencia a distancia, que impliquen una mayor eficiencia en la protección de la salud de las personas.

La telemedicina conlleva numerosos cambios en la manera de prestar los servicios sanitarios. Uno de los aspectos que cambian es la forma de manipular la información que se maneja. Su tratamiento resulta en el ámbito sanitario una actividad fundamental, siendo el empleo de datos concernientes a la salud imprescindible para desarrollar cualquier actividad sanitaria. Las nuevas tecnologías facilitan esta manipulación y abren la puerta a nuevas posibilidades. No cabe duda de que la facultad de comunicar información a cualquier lugar, en cualquier momento y de forma inmediata hace viables operaciones que son positivas en la tarea de salvaguardar la salud de la ciudadanía. Sin embargo, la creación de mayores y más ágiles flujos de información sanitaria

acentúa también otros riesgos. Entre ellos cabe destacar el peligro de que los datos se pierdan, se sustraigan, se alteren o se empleen de forma torticera. Es lógico pensar que en la medida en que el flujo de datos va a ser mayor y sean más las opciones de manipulación, sobre todo de puesta en común de los datos, mayor será también el riesgo de que se dé un mal uso de los mismos. Esta afirmación no es del todo cierta, pues si bien las nuevas tecnologías plantean nuevos peligros también plantean nuevas soluciones. Puede afirmarse que el uso del formato papel crea en general mayores problemas. Sea como sea, parece claro que ante la nueva dimensión que ha adquirido la información en las sociedades actuales cada vez hay una mayor concienciación de la ciudadanía en la necesidad de que se le garantice cierto control sobre sus datos. De esta manera, no hay duda de que todo sistema sanitario que se quiera presentar en la actualidad respetuoso o atento con los derechos fundamentales, deberá articular mecanismos para que ese control se garantice.

El derecho a controlar los datos de cada uno ha sido reconocido por gran parte de la doctrina e incluso por el TC, fundamentalmente a partir de la sentencia de 30 de noviembre del 2000 que resuelve la inconstitucionalidad de determinados apartados de la LOPD, como un derecho fundamental autónomo denominado derecho a la autodeterminación informativa o derecho a la protección de datos, incardinado en el artículo 18.4 CE. Este derecho está plenamente vigente en el ámbito sanitario. Sin embargo, la voluntad de cada uno de hacer lo que crea conveniente con los datos que le conciernen puede enfrentarse en ocasiones con otros intereses: desde el derecho a la protección de la salud del propio titular de los datos, de un tercero o de una colectividad, hasta intereses que tienen que ver con otros ámbitos extraños al sanitario, como son el derecho a la tutela judicial efectiva, la libertad de información o la seguridad nacional. La solución a la confrontación de estos derechos vendrá de la búsqueda de un equilibrio entre ellos, sin que ninguno quede anulado por completo.

El papel del Derecho es fundamental en la ponderación de estos intereses. El ordenamiento ha de tener como objetivo la búsqueda del equilibrio entre la necesidad de manipular datos sanitarios empleando las nuevas tecnologías, y la necesidad de proteger la intimidad y el derecho a la protección de datos de los usuarios de los sistemas sanitarios. La importancia de crear un marco jurídico adecuado deriva, sobre todo, de la relevancia de que los agentes que en el sector sanitario han de manipular los datos de carácter personal conozcan los parámetros en los que se deberán mover y cuál debe ser su comportamiento en cada situación.

En el ámbito estrictamente sanitario son numerosas las normas que se refieren a la intimidad e, incluso, a la protección de datos. Sin embargo, como ha subrayado repetidamente la doctrina, no existe una norma que específicamente regule la protección de datos en este sector, tal como lo hace en el ámbito internacional, aunque sea en términos generales, la Recomendación del Consejo de Europa sobre protección de datos médicos de 1997. La LBAP entra a regular algunos aspectos de esta materia, pero deja sin resolver otros muchos puntos. De esta forma, la determinación de los criterios que se han de seguir en la manipulación de datos sanitarios derivará de la interpretación conjunta de la normativa de protección de datos y la normativa sanitaria. Este ejercicio de interpretación no resulta tarea sencilla, fundamentalmente por el gran número de normas que se manejan y por la complicada relación entre ellas. Desde directivas

europeas hasta protocolos de actuación que tienen aplicación en el ámbito interno de centros concretos, pasando por convenios y recomendaciones del Consejo de Europa, leyes y reglamentos que tienen aplicación en el ámbito estatal o autonómico, son innumerables las normas que afectan a esta materia. Además, en ocasiones las leyes se remiten las unas a las otras o recogen contenidos contradictorios. La interpretación conjunta de todas estas normas resulta una labor complicada. La normativa de protección de datos reconoce una serie de principios y derechos que han de aplicarse al ámbito sanitario. Como se ha puesto de manifiesto en numerosas resoluciones e informes de las distintas agencias de protección de datos, esta aplicación no es tarea fácil por la especial complejidad que presenta la actividad sanitaria.

Lo que en este trabajo interesa es la protección de los datos de carácter personal sanitarios. Se trata de datos de salud, entendido este concepto en un sentido amplio, como cualquier información que se refiera o se vincule a realidades de las que pueda deducirse el estado físico o mental de una persona, empleados en un ámbito concreto, como es el sanitario. La normativa de protección de datos se aplicará cuando estos datos se sometan a tratamiento o manipulación, bien sea automatizado o manual.

Como punto de partida la protección que la LOPD otorga en el artículo 7 a los datos de salud es especial. La consideración de estos datos como sensibles hace que la Ley les reconozca un régimen de salvaguarda más estricto o riguroso en comparación al dado a otros datos. Se han aportado diferentes teorías sobre los motivos que llevan al legislador a aplicar tal régimen, pero parece acertado afirmar que esa consideración especial se fundamenta en el hecho de que un mal empleo de los datos sanitarios puede tener unos efectos especialmente perjudiciales para los titulares de los datos. No hay más que pensar en las consecuencias que puede tener, por ejemplo, que la referencia sobre la condición de una persona como seropositiva sea conocida en ámbitos como el laboral o el social. Sin embargo, si bien el punto de partida es la protección rigurosa de estos datos de salud, el ordenamiento flexibiliza este régimen dependiendo de las circunstancias en que la información se esté manipulando. De esta forma en el ámbito sanitario el derecho a la autodeterminación informativa deberá ceder en muchas ocasiones en beneficio de otros intereses.

Partiendo de esta premisa el régimen de protección de los datos sanitarios tiene en cuenta diferentes aspectos. A) Primero, todo tratamiento de estos datos debe respetar los denominados principios de calidad, recogidos en el artículo 4 de la LOPD. Se trata de una suerte de principios generales que toda manipulación ha de respetar, y que se concretan en el principio de finalidad, de pertinencia y de veracidad.

En primer lugar, el principio de finalidad exige, atendiendo a la interpretación que la jurisprudencia y determinada doctrina ha realizado, que los datos recabados para conseguir un objetivo determinado, concreto y legítimo no podrán emplearse para un fin distinto al que motivó la recogida, a no ser que medie el consentimiento del titular de los datos o una habilitación legal. En el ámbito sanitario la finalidad principal que se persigue con la manipulación de datos no es otra que la protección de la salud. Se plantea, por lo tanto, si la capacidad de controlar los datos de cada uno puede verse limitada con el fin de proteger la salud; por ejemplo, si se pueden

manipular esos datos sin recabar el consentimiento del titular. La protección de la salud se recoge en la CE como principio rector de la política social y económica y no como un derecho fundamental, por lo que podría ponerse en duda la posibilidad de que este principio rector pudiera tener suficiente entidad como para erigirse en límite del derecho fundamental a la autodeterminación informativa. En la actualidad no parece haber dudas al respecto: en términos genéricos el derecho a la protección de la salud puede constituirse en límite del derecho fundamental a la protección de datos. El concepto de derecho a la protección de la salud, sin embargo, abarca un campo de realidad amplio compuesto por multitud de acciones: asistencia sanitaria, investigación, estadísticas, gestión administrativa y económica, inspección, docencia, seguridad alimentaria, etc. Cuando se dice que unos datos van a ser empleados con el fin de salvaguardar la salud habrá que concretar a cuál de estas acciones se está haciendo referencia, pues el régimen jurídico a aplicar será diferente cuando se trate de una o de otra. El cumplimiento del principio de finalidad exigirá, por lo tanto, que se especifique el fin concreto que se persigue a efectos de aplicar el contenido de la normativa de protección de datos.

En segundo lugar, el principio de pertinencia requiere, como expresión del genérico principio de proporcionalidad, que, una vez definido el objetivo concreto que se pretende con el tratamiento de información, no se empleen datos que no sean adecuados, ni necesarios, ni estrictamente proporcionales para la consecución de dicho fin. La adecuación hace referencia a la obligación de que los datos concretos que se manipulen sirvan desde un punto de vista científico o empírico para el cumplimiento de los fines. Si el tratamiento de unos datos concretos no trae como resultado la protección de la salud de un paciente en una situación determinada, se entenderá que el uso de esa información no será adecuado. La necesidad reconoce la obligación de manipular sólo los datos que sean estrictamente necesarios para conseguir el objetivo, dejando a un lado el tratamiento de datos que, si bien pueden servir para conseguir el fin, su uso no es necesario debido a que los efectos negativos que genera son mayores que los positivos. La proporcionalidad en sentido estricto simplemente requiere que el tratamiento de los datos esté justificado desde el punto de vista jurídico para la consecución del objetivo pretendido. En este sentido la LOPD constituye base jurídica suficiente para entender que la protección de la salud puede ser un fin que limite el derecho a la autodeterminación informativa. En términos genéricos el cumplimiento del principio de pertinencia llevará a tener que analizar si el uso de cada uno de los datos está justificado en el cumplimiento del fin de proteger la salud y si para ello es necesario que la información a tratar aparezca asociada o es posible su disociación. Lo que se pretende en última instancia es que la autodeterminación informativa se vea afectada de la menor manera posible con el tratamiento de datos que se va a llevar a cabo. Sin embargo, desde un punto de vista práctico este principio no podrá suponer la limitación de la capacidad de acción de los profesionales sanitarios. Es decir, si bien sólo se pueden emplear los datos estrictamente necesarios, el profesional deberá contar con toda la información necesaria. Ante la duda, parece conveniente apostar por el principio de que es mejor que el profesional cuente con más información de la estrictamente necesaria, pues en caso contrario las consecuencias podrían llegar a ser especialmente negativas desde la perspectiva de la protección de la salud.

Por último, el principio de veracidad exige que la información que se manipule sea siempre veraz, completa, exacta y actualizada. Los datos que no cumplen con estos requisitos serán

cancelados en la medida en que no servirán para cumplir con la finalidad pretendida. En el ámbito sanitario, sin embargo, la obligación de cancelar los datos del pasado, no actualizados, debe flexibilizarse. En este sector contar con información del pasado resulta especialmente útil para la consecución de diversos fines, tanto asistenciales como de investigación y otros, lo que lleva a que la propia normativa sanitaria se preocupe por disponer la obligación de conservar muchos de los documentos que se emplean durante cierto periodo de tiempo.

El cumplimiento de los principios de calidad debe hacerse caso por caso atendiendo a las circunstancias que rodean a cada tratamiento de datos. Sin embargo, como referencia a seguir han de tenerse en cuenta las disposiciones generales que crean los ficheros sanitarios. Los ficheros de las administraciones públicas han de crearse a través de disposiciones generales. En estas disposiciones se fijan los datos que se van a manipular, los fines concretos a los que se van a destinar, los posibles destinatarios de los datos, etc. Y, si bien es cierto que en la práctica los conceptos que se emplean en estas disposiciones son muy genéricos, dejando amplios márgenes de actuación a los responsables de ficheros, lo cierto es que constituyen una buena referencia para determinar los parámetros entre los que se van a tratar unos datos y ver en qué medida se cumplen en la práctica los señalados principios.

B) Como segundo principio a respetar la normativa de protección de datos regula el consentimiento informado. De inicio todo tratamiento de datos ha de estar fundamentado o justificado en la autorización del titular, que tiene libertad para decidir qué hacer con ellos. Si el derecho a la autodeterminación informativa constituye la facultad de una persona de controlar lo que sucede con sus datos, una concreción de esa facultad será la capacidad de esa persona de consentir o no el tratamiento de la información que otra persona pretende. Hoy día el principio de autonomía aparece especialmente enraizado en el ámbito sanitario como criterio que ha de informar en todo momento la relación entre los profesionales sanitarios y los usuarios. La autonomía supone que el usuario del sistema sanitario tendrá una mayor participación en la toma de decisiones en cuestiones que afectan, tanto a la protección de su salud como de sus datos. El consentimiento informado no es más que la concreción de esa autonomía.

Esta figura se compone de dos principios o derechos diferentes que, sin embargo, están íntimamente relacionados. Se trata del derecho a ser informado y del derecho a consentir. La relación entre ambos es evidente, por cuanto que para consentir un tratamiento es necesario previamente ser informado de las características que va a tener. No se puede autorizar lo que se desconoce. Sin embargo, tal como hace la LOPD, merecen un análisis separado.

El derecho a ser informado, regulado en el artículo 5 de la Ley, recoge la facultad del titular de conocer los parámetros que van a rodear al tratamiento de sus datos: la finalidad que se persigue, los destinatarios, los derechos del titular de los datos, la identidad y dirección del responsable, etc. La normativa de protección de datos reconoce, además, la posibilidad de limitar este derecho en determinados supuestos. Dependiendo de si los datos han sido recogidos del propio titular o de una fuente distinta, se exceptúa el derecho, en el primer caso, si el contenido de la información es deducible de la naturaleza de los datos a tratar o de las circunstancias en que se recogen; y, en el segundo, si así lo prevé una Ley, el tratamiento tiene fines históricos,

científicos o estadísticos o el ejercicio del derecho a la información supone a criterio de la agencia de protección de datos correspondiente un esfuerzo desproporcionado o resulta imposible para el responsable. En ocasiones se han pretendido aplicar estas excepciones en el ámbito sanitario. Esta posibilidad hay que analizarla con cautela. Se entiende aquí que la información ha de tener como punto de partida una vigencia general en este sector. Sin embargo, a esta idea hay que contraponerle el principio de que el ejercicio del derecho a la información no puede ser obstáculo insalvable a la hora de realizar la labor de los profesionales. En este sentido, no es asumible que en cada acto asistencial el facultativo informe al paciente sobre los citados elementos. Esto no quiere decir que la información no pueda llevarse a cabo. La información ha de darse siempre que se pueda y de la forma más completa posible. Para ello es necesario emplear todos los mecanismos a disposición del responsable del fichero. El uso de tablones de anuncios, el envío de cartas informativas, el uso de folletos, la remisión de e-mails, etc. supondrán instrumentos que ayuden a informar, aunque sea de manera genérica, sobre las circunstancias que rodearán el tratamiento de los datos sanitarios. Esta información genérica abarca la mayoría de operaciones que se realizan en el ámbito sanitario. Si lo que se va a llevar a cabo es un acto distinto a esas operaciones comunes, caso de una investigación sobre una determinada patología, será necesaria, salvo que quepa la aplicación de una excepción, una información concreta sobre el uso específico que se va a dar a los datos.

El derecho a otorgar el consentimiento, por su parte, es la facultad de autorizar de manera inequívoca, libremente, y una vez se ha sido informado de forma expresa, un tratamiento de datos. El consentimiento ha de ser emitido sobre un objeto determinado y conocido por el titular de los datos. Además, cuando se trata del tratamiento de datos de salud la LOPD exige en su artículo 7.3 que la autorización sea expresa, sin que baste un consentimiento tácito.

En el ámbito sanitario cuando una persona acude a recibir asistencia sanitaria remite la información que se le solicita de forma voluntaria, bien sea al facultativo o al personal administrativo correspondiente. Difícilmente puede obligarse, empleando incluso la fuerza, a un sujeto a que facilite información sobre su salud. Sin embargo, una vez los datos obran en los ficheros sanitarios, fundamentalmente en las historias clínicas, su uso puede llevarse a cabo, en la mayoría de casos, sin necesidad de recabar la autorización del titular. Los artículos 7.6 y 8 de la LOPD constituyen base jurídica suficiente para entender que se exceptúa la necesidad de recabar el consentimiento del titular cuando la manipulación de datos tiene como fin la asistencia sanitaria, la prevención médica o la gestión sanitaria. Las referencias en la normativa sanitaria a que los profesionales de la sanidad han de tener acceso a la documentación clínica también apoyan esta afirmación. Si bien es cierto que dependiendo de la concreta función de que se trate, pues no es lo mismo la asistencia médica que una investigación o la realización de una estadística, el régimen jurídico es distinto, parece posible apoyar la idea de que en términos genéricos el derecho a la autodeterminación informativa cede ante el derecho a la protección de la salud. Esta conclusión responde a la necesidad de que en este ámbito la información pueda fluir de forma ágil por los sistemas de información, y que un bien jurídico tan importante como la protección de la salud no dependa de la voluntad de los titulares de los datos de que no se manipule su información. Hay que tener en cuenta que a la hora de proteger la salud de las personas no se puede conocer la situación o condición física o mental de alguien sin que se

tenga acceso a los datos que muestran esta situación. Sujetar al consentimiento del titular el acceso a dichos datos supone inhabilitar a los profesionales en la realización de su trabajo y anular la posibilidad de que se proteja la salud de las personas. Otra cosa será que, una vez conozca su condición, el paciente acepte o no un tratamiento sanitario.

C) Los citados principios de calidad y el consentimiento informado constituyen, sin duda, los elementos más destacados que componen el derecho a la autodeterminación informativa. Sin embargo, más allá de estas figuras, la normativa de protección de datos regula, en el apartado dedicado a los principios de la protección de datos, otra serie de puntos que tienen también su importancia. Cabe destacar la regulación que las normas hacen de los diferentes supuestos de transmisión de datos. La LOPD entra a regular en diferentes preceptos todos los casos en que los datos que están siendo manipulados por un responsable del fichero salen de su esfera de control y son transferidos a otra persona o al público en general: desde los casos en que el responsable transmite la información de carácter personal a otro sujeto, caso de la cesión, del acceso a los datos por un tercero o las transferencias internacionales, hasta los supuestos en que los datos simplemente salen a la luz sin un destinatario concreto, que es lo que sucede cuando se vulnera el deber de secreto. La necesidad de regular estas operaciones es evidente, pues se trata de las manipulaciones que generan mayores riesgos para el derecho fundamental a la autodeterminación informativa. En estos casos los datos que inicialmente están siendo tratados por un responsable concreto, que normalmente es conocido por el titular de los datos, salen del ámbito de relación entre el titular y ese responsable para situarse en la esfera de control de otras personas, bien sea un tercero determinado o del público en general. Los riesgos que generan las transmisiones de datos son principalmente dos: primero, la posibilidad de que distinta información sobre una misma persona recale de distintas fuentes en un mismo fichero, con el riesgo de que se cree un perfil completo de las personas; y, segundo, la posibilidad de que las transmisiones se sucedan de tal manera que el titular de los datos transferidos pierda la referencia sobre quién es el responsable del fichero, sobre todo, a efectos de exigir responsabilidades. Estos riesgos se acentúan cuando la información que se transmite es especialmente sensible, caso de los datos de salud, por los efectos que tendría una manipulación inadecuada de los mismos.

Son distintas las fórmulas a través de las cuales se pueden transmitir los datos: la vulneración del deber de secreto, la cesión, el acceso a los datos por cuenta de terceros y las transferencias internacionales. La regulación del acceso a los datos sanitarios por cuenta de terceros responde a la necesidad de articular mecanismos que garanticen la protección de la autodeterminación informativa cuando se dan supuestos de *outsourcing* o externalización de determinados servicios. En el ámbito sanitario, al igual que en otras esferas de la realidad, no es extraño que algunos servicios se externalicen. Muchas veces esta operación exige que sujetos extraños a la Administración sanitaria con la que los usuarios tienen relación directa tengan que tener acceso a los datos de dichos usuarios. Para que este acceso se realice de manera segura y respetuosa con el derecho a la protección de datos, el ordenamiento exige que se formalice un contrato entre la Administración responsable del servicio y el sujeto encargado de llevar a cabo materialmente dicho servicio. En este contrato se deberán establecer las condiciones en que el encargado

podrá acceder a los datos para ejecutar el servicio. El acceso a datos por cuenta de terceros no plantea excesivos problemas interpretativos desde la perspectiva sanitaria.

La transferencia internacional plantea mayores interrogantes. Cada vez son más las transmisiones de datos sanitarios a terceros países. En principio, la existencia de un flujo internacional de datos sanitarios puede verse de forma positiva por cuanto facilita, por ejemplo, una adecuada asistencia en cualquier punto del globo o la realización de estudios epidemiológicos contando con más recursos o instrumentos. La posibilidad, sin embargo, de que los datos de salud de la ciudadanía puedan acabar en ficheros situados en países que no cuentan con un sistema de protección de datos equiparable al interno genera dudas e inseguridad. De inicio, la normativa de protección de datos dispone un régimen jurídico que garantiza la seguridad en la realización de estas transferencias, distinguiendo si la operación se va a realizar a un país que presenta un nivel de protección adecuado o no. El problema tiene su origen en el momento en que la LOPD reconoce la posibilidad de no aplicar este régimen jurídico de protección cuando las transferencias se realicen, entre otros supuestos, para la prevención o diagnóstico médico, asistencia sanitaria o gestión de servicios sanitarios, pues una interpretación amplia de estos conceptos podría llevar a abrir la puerta a la creación de un flujo incontrolado de datos de salud de alcance internacional, incluso por países que no cuentan con un sistema de protección de datos adecuado. Se apuesta aquí por una interpretación no excesivamente amplia de los conceptos señalados, que si bien permite la transmisión de datos de salud sin aplicar mayores garantías cuando se trata de finalidades asistenciales o de investigaciones directamente vinculadas con la protección de la salud colectiva, no hace lo mismo con otros fines, como los puramente administrativos.

La fórmula más común de transmitir los datos de salud la constituye la cesión de datos. La comunicación de la información puede venir justificada bien porque lo autoriza el titular de los datos o bien porque existe una causa que justifica la transmisión. La normativa de protección de datos reconoce múltiples supuestos en que el derecho a consentir las cesiones se ve exceptuado. A pesar de que el ordenamiento no se refiera concretamente a este aspecto, estando los datos de salud sujetos a una especial protección por la Ley, es lógico pensar que de todos esos supuestos sólo algunos son aplicables a las comunicaciones de los datos sanitarios. En primer lugar, en el ámbito estrictamente sanitario, la protección de la salud parece ser un bien jurídico de suficiente entidad para justificar la excepción al consentimiento y configurar flujos de información que faciliten la labor de los profesionales sanitarios. Hay que tener en cuenta que la cada vez mayor especialización dentro de los sistemas sanitarios, tanto en los propios centros como en las distintas administraciones que están vinculadas a la materia de la salud, lleva a que se creen distintas áreas de acción con sus propios ficheros. Muchas veces, diferentes áreas han de relacionarse para ofrecer determinado servicio de asistencia o de investigación, teniendo que acceder personal de uno y otro departamento a los ficheros del otro. Hacer depender la ejecución de estas cesiones de la voluntad de los usuarios haría sujetar el buen funcionamiento de la Administración sanitaria a la voluntad de los pacientes, lo cual no parece que esté en la voluntad del legislador, cuando, sobre todo, en la normativa sanitaria reconoce la necesidad de que los profesionales tengan acceso a la documentación clínica y crea cada vez más mecanismos de transmisión de datos entre distintas instituciones en ámbitos como la epidemiología o la

farmacovigilancia. En segundo lugar, los datos de salud pueden cederse fuera del ámbito sanitario. Partiendo de una interpretación conjunta de la LOPD, la LBAP y normativa sectorial que regula materias tan variadas como el funcionamiento de la institución del Defensor del Pueblo, de los seguros, los medios de comunicación, derecho de acceso a la información obrante en las administraciones o, especialmente, el funcionamiento y organización del poder judicial, puede llegarse a la conclusión de que en determinados casos es posible sacar los datos sanitarios de su lugar común de manipulación con el fin de satisfacer otros intereses. Muchas veces se ha cuestionado desde diversas instancias en qué casos y cumpliendo qué condiciones pueden transmitirse los datos de salud fuera del ámbito estrictamente sanitario. Lo cierto es que la normativa sanitaria y la reguladora de la protección de los datos de carácter personal no llevan a cabo regulaciones lo suficientemente claras y específicas sobre esta cuestión, por lo que la solución debe venir del análisis de la citada normativa sectorial. El problema que se genera en la práctica es el vacío que en estas normas rige, también, como norma general, sobre esta cuestión. A pesar de que cada vez son más las normas reguladoras de las más diversas materias que tienen en cuenta la perspectiva de la protección de datos, todavía hoy es común la falta de regulación sobre esta realidad. De esta forma, se concluye que si bien es posible encontrar en la normativa sectorial base jurídica que justifique la transmisión de datos sanitarios a distintos destinatarios con los citados fines, la interpretación de esa normativa deberá realizarse siempre con cautela.

D) En un apartado distinto al dedicado a los principios de la protección de datos la LOPD regula los derechos de las personas. Entre estos derechos pueden destacarse en lo que afecta al sector sanitario los de acceso, cancelación, rectificación, oposición, indemnización y el derecho a impugnar valoraciones. Este cuerpo de facultades constituye uno de los contenidos más relevantes del derecho a la autodeterminación informativa. Se ha repetido que este derecho no es otra cosa que la facultad de controlar lo que sucede con los datos de cada uno desde una perspectiva negativa, de defensa ante actos de terceros, y positiva, de acción del propio titular de los datos. Esta segunda perspectiva se concreta en el citado elenco de facultades, que permiten al titular llevar a cabo diferentes acciones de control activo de los datos.

De esos derechos los que, sin duda, mayores problemas plantean en el ámbito sanitario son los de acceso, cancelación y rectificación. El derecho de acceso se refiere a la facultad del titular de conocer los datos que sobre su persona se están manipulando en la Administración sanitaria correspondiente, su origen y las operaciones que se vayan a realizar con ellos. En principio, este derecho tiene plena vigencia en el ámbito sanitario, debiendo facilitarse, además, tal como exigen la LOPD y el reglamento que la desarrolla, el procedimiento para hacerlo efectivo. La importancia del derecho de acceso en el ámbito sanitario reside no sólo en que constituye una facultad por la que el titular de los datos controla lo que sucede con los mismos, sino porque de esta manera conoce información sobre su estado de salud, más allá de la que pueda conocer en atención al ejercicio del derecho a la información recogido en la normativa sanitaria, a la hora de poder tomar decisiones. No obstante, a este derecho también se le imponen en la normativa diferentes limitaciones. Concretamente, y dejando a un lado los límites dispuestos en la LOPD, las normas que regulan la actividad sanitaria señalan que el titular de los datos no podrá ejercer el acceso a la documentación clínica que le corresponde cuando estén en juego la intimidad de

terceras personas, cuando en la documentación haya anotaciones subjetivas de los facultativos o, habría que añadir, cuando el acceso pueda perjudicar al paciente. El primero y último de los supuestos no han planteado mayores problemas de interpretación en la doctrina, sin embargo, el límite al acceso basado en la existencia de anotaciones subjetivas ha creado cierto debate de no fácil solución. Limitar, tal como hace la LBAP, sin mayor matiz, un derecho fundamental como es el de autodeterminación informativa basándose en un supuesto derecho a la propiedad intelectual de los profesionales sanitarios sobre las anotaciones o en su derecho a la intimidad, plantea muchas dudas. A pesar de que algunas normas y protocolos de actuación han tratado de matizar el contenido de este límite, se interpreta aquí que su virtualidad ha de cuestionarse, más teniendo en cuenta las dificultades que plantea su aplicación en la práctica.

Los derechos de cancelación y rectificación presentan también sus particularidades en el ámbito sanitario. El derecho de rectificación reconoce la facultad de modificar el contenido de una información cuando no se corresponde con la realidad, bien porque es errónea, incompleta o porque no está actualizada. El derecho de cancelación va más allá. Según la Ley, la cancelación implica, primero, el bloqueo de los datos y, después, su supresión. En cualquier caso, supone que unos datos no se puedan seguir manipulando por un responsable de fichero. Se cancelan los datos que no sirven para cumplir el fin que se pretende. Ambos derechos tienen una relevancia especial pues consiguen que los datos a manipular respondan siempre a la realidad actual, de forma que se garantice el cumplimiento de la finalidad que se persigue, en este caso, la protección de la salud. Su sentido responde a la necesidad de que se cuente en todo momento con información veraz. El ejercicio de estos derechos en el ámbito sanitario plantea problemas prácticos de envergadura. La rectificación de los datos sanitarios erróneos supone una acción necesaria para poder asistir adecuadamente a los pacientes. El problema reside en que la información sanitaria es la mayoría de veces de difícil comprensión para el ciudadano común y se basa en muchas ocasiones en valoraciones, opiniones o perspectivas profesionales subjetivas de una enfermedad, o estado físico o mental. Tratar de rectificar este tipo de información puede plantear problemas prácticos y es por ello que se estima necesaria una estrecha colaboración, en todo momento, entre el titular de los datos que pretende rectificar la información y los profesionales sanitarios, que comprenden la información sanitaria de manera adecuada. Por su parte, el derecho de cancelación se enfrenta en el ámbito sanitario al deber que impone la normativa sanitaria de conservar la documentación clínica durante un plazo determinado. La obligación de conservar se reconoce en las leyes para diferentes documentos, entre los que está la historia clínica, para el cumplimento de los más diversos fines, fijando en algunos casos una obligación de conservación indefinida. Este deber de conservar plantea el riesgo de que en la práctica se cree un almacén de datos, con el peligro que ello conlleva de que esa información se pierda, se filtre, sea mal empleada, etc. Es por ello que si bien puede asumirse que haya datos que deben ser conservados de manera indefinida, deberán respetarse en todo caso los principios de calidad, garantizando así que sólo se guardan los datos estrictamente necesarios para el cumplimiento de los objetivos citados y disociando, siempre que sea posible la información.

De todo lo dicho puede concluirse que la manipulación de datos de salud en el ámbito sanitario plantea una serie de cuestiones que todavía hoy no han sido resueltas definitivamente por el legislador. La actividad sanitaria requiere del tratamiento constante de información y los

profesionales sanitarios no pueden encontrarse ante la inseguridad que genera la inexistencia de un marco jurídico claro y preciso sobre esta cuestión. Sin embargo, la realidad es que el ordenamiento jurídico actual se acerca mucho a esa situación y dista mucho de ser un marco completo y claro. Ni la Directiva europea de protección de datos, ni la LOPD, ni el reglamento que desarrolla la Ley, ni tan siquiera la LBAP, entran a concretar cómo se limita el derecho a la autodeterminación informativa en el ámbito sanitario, ni indican criterios mínimamente claros sobre cómo se puede cumplir la normativa de protección de datos en el sector sanitario. La escasa jurisprudencia existente sobre esta materia tampoco aclara excesivamente las interrogantes planteadas. A pesar de ser una máxima repetida constantemente por quienes han entrado a analizar esta materia no está de más subrayar que el Derecho va, otra vez, por detrás de la realidad. La necesidad de una norma concreta que entre a regular la protección de datos sanitarios se entiende hoy día, cuando la telemedicina se encuentra en un estadio de desarrollo relativamente avanzado, evidente. Esta norma deberá tratar de cohonestar la LOPD y la LBAP con el fin de concretar los criterios básicos que deberán seguirse en la manipulación de datos en el ámbito sanitario, y determinar en qué medida y con qué límites permanecen vigentes los principios y derechos citados en este ámbito y de qué forma se pueden ejercer estos derechos. Saber si se ha de llevar a la práctica la obligación de informar y, en caso afirmativo, cómo, o conocer si es necesario recabar el consentimiento del titular para manipular los datos y, hasta dónde llegan los límites a este derecho a consentir, etc. es necesario para poder desarrollar la actividad sanitaria con eficiencia. La inseguridad jurídica a la que el actual ordenamiento aboca a juristas, ciudadanía y, sobre todo, profesionales de la sanidad no ayuda a este fin. Se ha tratado de aportar aquí un poco de luz sobre una materia en la que todavía son numerosas las cuestiones a resolver. Las conclusiones que se han ido extrayendo en los distintos apartados derivan de una interpretación conjunta de la normativa de protección de datos y las normas que regulan el funcionamiento y organización del sector sanitario, y tratan de encontrar cierto equilibrio entre los distintos intereses y derechos que entran en juego cuando se manipulan datos de carácter personal en el ámbito sanitario. Evidentemente, estas conclusiones pueden ser debatidas partiendo de un enfoque distinto de las señaladas normas.

BIBLIOGRAFÍA.

ABEL LLUCH, Xavier, "El derecho de información del paciente como presupuesto del consentimiento informado. Su régimen jurídico en la Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información Documentación Clínica", VVAA, *El juez civil ante la investigación biomédica*, Cuadernos de Derecho Judicial, Madrid, 2004.

ABRAMOVICH, Victor y COURTIS, Christian, *Los Derechos Sociales como Derechos Exigibles,* Trotta, Madrid, 2002.

ACED FÉLEZ, Emilio, "La protección de datos en la cooperación policial europea: de la Recomendación (87) 15 al principio de disponibilidad", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

ACOSTA GALLO, Pablo, "Administración electrónica: ¿Existe un derecho fundamental a la protección de datos personal?", *RGDA,* nº 15, 2007. En http://www.iustel.com

ACOSTA RAMÍREZ, Miguel, "Estudio Práctico sobre el Principio de Consentimiento en el marco de la Normativa sobre Protección de Datos de Carácter Personal: el caso RACC (2006)", *REPD,* nº 1, 2006.

ACUÑA, Berta, "Receta Electrónica en la Comunidad Autónoma de Galicia"*, IyS*, nº 36, mayo 2002, http://www.seis.es/.

AGIRREAZKUENAGA, Iñaki y CHINCHILLA, Carmen, "El Uso de Medios Electrónicos, Informáticos y Telemáticos en el Ámbito de las Administraciones Públicas", *REDA*, nº 109, 2001.

AGUADO CORREA, Teresa, *El Principio de Proporcionalidad en Derecho Penal*, Edersa, Madrid, 1999.

AGUADO I CUDOLÁ, Vicenç, *Derecho de la Seguridad Pública y Privada,* Thomson Aranzadi, Cizur Menor, 2007.

AGÚNDEZ FERNÁNDEZ, Antonio, *Ley 29 de 13 de julio de 1998 del Proceso Contencioso-Administrativo. Comentarios y Jurisprudencia*, Comares, Granada, 2000.

AGÚNDEZ LERÍA, Irene Mª, "Principios relativos a la Calidad de los Datos", ZABÍA DE LA MATA, Juan (Coord.), *Protección de Datos. Comentario al Reglamento*, Lex Nova, Valladolid, 2008.

AIBAR, Eduard y URGELL, Ferran, *Estado, Burocracia y Red. Administración electrónica y cambio organizativo,* Ariel, Barcelona, 2007.

ALAMILLO DOMINGO, Ignacio, “La identidad electrónica en la red”, RALLO LOMBARTE, Artemi y MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Derecho y Redes Sociales,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

ALARCÓN SOTOMAYOR, Lucía, *El Procedimiento Administrativo Sancionador y los Derechos Fundamentales,* Thomson-Civitas, Cizur Menor, 2007;

-*La garantía non bis in idem y el procedimiento administrativo sancionador,* Iustel, Madrid, 2008.

ALEXY, Robert, *Teoría de los Derechos Fundamentales, Centro de Estudios Constitucionales*, Madrid, 1997.

ALMUZARA ALMAIDA, Cristina, “Relaciones Precontractuales y Contractuales”, LESMES SERRANO, Carlos (Coord.), *Estudio Práctico sobre la Protección de Datos de Carácter Personal,* Lex Nova, Valladolid, 2007;

-“Ficheros Privados con régimen especial. Solvencia Patrimonial y Crédito”, LESMES SERRANO, Carlos (Coord.), *Estudio Práctico sobre la Protección de Datos de Carácter Personal*, Lex Nova, Valladolid, 2007.

ALONSO LÓPEZ, Fernando A. (Coordinador), “Informatización en Atención Primaria”*,* http://www.semfyc.es/

ALONSO LÓPEZ, F. A., y GANZEDO GONZÁLEZ, Z., “Informatización Integral de la Atención Primaria”*, Formación Médica Continuada*, vol. 6, nº 5, 1 mayo 1999, http://www.doyma.es/

ALONSO MARTÍNEZ, Carlos, “Aproximación a Determinados Conceptos del RD 994/1999 de 11 de junio, sobre Medidas de Seguridad*”, AIA*, nº 35, abril 2000.

ALONSO OLEA, Manuel y FANEGO CASTILLO, Fernando, *Comentario a la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica*, Thomson-Civitas, Madrid, 2003

ÁLVAREZ CIENFUEGOS, José María, “Confidencialidad del Dato Sanitario, Derechos de los Pacientes e Intereses Generales”*,* II Congreso Nacional de Derecho Sanitario, 23-25 noviembre 1995;

-“La Naturaleza de la Actividad Administrativa Sanitaria y su Régimen Jurídico. Apertura de Hospitales y Clínicas”, GÓMEZ Y DÍAZ CASTROVERDE, José (Dir.), *Lecciones de Derecho Sanitario*, Universidade da Coruña, A Coruña, 1999;

-“La Aplicación de la Firma Electrónica y la Protección de Datos de Salud”*, AIA*, nº 39, abril 2001.

ÁLVAREZ DE NEYRA KAPPLER, Susana, *La Prueba de ADN en el proceso penal,* Comares, Granada, 2008.

ÁLVAREZ RICO, Manuel, "Informática y Derecho en España", *IyD*, nº 23-26, UNED, 1998.

ÁLVAREZ RIGAUDIAS, Cecilia, "Transferencias internacionales de datos", PALOMAR OLMEDA, Alberto (Coord.), *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre),* Thomson- Civitas, Cizur Menor, 2008;

-"Las transferencias internacionales de datos personales", PALOMAR OLMEDA, Alberto (Coord.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

ALLENDE, Oscar, "Informática: el Abuso de su Poder"*,IyD*, nº 4, UNED, 1994.

AMENGUAL PLIEGO, Miguel, "Información científica, Internet y nuevas tecnologías", *SEMERGEN* nº 30, 2004, http://www.doyma.es/.

ANDÉREZ GONZÁLEZ, Alberto, "Historia Clínica e Informática: Aspectos Legales (I)", *Informática y Salud*, nº18, noviembre-diciembre, 1998, http://www.seis.es/;

-"Aspectos Legales de la Historia Clínica Informatizada", ponencia presentada en el seminario *Innovaciones en Tecnologías de la Información de la Salud*, Segovia 19-20 de septiembre 2002, http://www.conganat.org/seis/

ANDRÉS PÉREZ, María del Rocío, *El Principio de Proporcionalidad en el Procedimiento Administrativo Sancionador*, BOSCH, Barcelona, 2008.

ANTEQUERA VINAGRE, José María, "Historia Clínica e Instrucciones Previas", en http://www.diariomedico.com;

-"Una nueva era en la sanidad. El ciudadano sanitario", *Revista de Administración Sanitaria siglo XXI,* vol. 1, nº 2, 2003, en http://www.doyma.es/.

ANTÓN BARBERÁ, Francisco y SOLER TORMO, Juan Ignacio, *Administración Policial. Legislación e Investigación privada,* Tirant lo Blanch, Valencia, 2000.

APARICIO SALOM, Javier, *Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal,* Aranzadi, Navarra, 2000;

-Estudio sobre la Ley Orgáncia de Protección de Datos de Carácter Personal, Aranzady y Thomson-Reuters, Cizur Menor, 2009;

-"La calidad de los datos", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal"*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

APARISI MIRALLES, Ángela, “El significado del Principio de la Dignidad Humana: un análisis desde la Ley 41/2002 sobre derechos de los pacientes”, LEÓN SANZ, Pilar (ed.), *La implantación de los Derechos de los Pacientes*, EUNSA, Pamplona, 2004.

APDCM, *Manual de Datos para las Administraciones Públicas*, Thomson-Civitas y APDCM, Madrid, 2003;

-*Guía de Protección de Datos Personales para Servicios Sanitarios Públicos,* Thomson-Civitas y APDCM, Madrid, 2004;

-*Protección de datos personales para Servicios Sanitarios Públicos*, Thomson-Civitas y APDCM, Madrid, 2008.

ARENAS RAMIRO, Mónica, *El Derecho Fundamental a la Protección de Datos Personales en Europa*, Tirant lo Blanch, Valencia, 2006;

-“El Principio del Consentimiento en los Estados miembros de la Unión Europea”, *REPD,* nº 2, 2007;

-“La Sentencia del Tribunal Supremo de 19 de septiembre de 2008: protección de datos personales y apostasía”, *REPD,* nº 4, 2008;

-“El derecho de acceso”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

ARIAS MÁIZ, Vicente, “Una excepción al principio del consentimiento informado no contemplada en el artículo 6 LOPD: el uso de datos personales por medios de comunicación”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

ARIÑO ORTIZ, Gaspar y SOUVIRÓN, José Mª, *Constitución y colegios profesionales,* Unión Editorial, Madrid, 1984.

ARQUILO COLET, Begoña, *Seguro y responsabilidad patrimonial de la Administración Pública*, Atelier, Barcelona, 2008.

ARROYO i AMAYUELAS, Esther, *La Protección al Concebido en el Código Civil*, Civitas, Madrid, 1992.

ARROYO YANES, Luis Miguel, “La Cancelación de Datos Personales en Ficheros de Titularidad Pública en el Proyecto de LORTAD”, *IyD,* nº 4, Actas del III Congreso Iberoamericano de Informática y Derecho, UNED, Mérida, 1994;

-“Las Administraciones Públicas y la excepción al principio de prestación del consentimiento por parte del interesado a la recogida y tratamiento de sus datos personales”, TRONCOSO

REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

ARRUEGO, Gonzalo, "La Naturaleza Constitucional de la Asistencia Sanitaria no consentida y los denominados supuestos de <<Urgencia Vital>>", *REDC*, nº 82, 2008.

ARTAL, Roser, "La informatización de los datos de salud", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud,* APDCat y Marcial Pons, Madrid y Barcelona, 2006.

ARZA, Enrique G. y GRANDES ODRIOZOLA, Gonzalo, "¿Podemos Superar las Dificultades de Acceso a la Información Científica en Atención Primaria?", Comunicación presentada en Infors@lud-net 98, 24-27 marzo 1998, http://www.seis.es/.

ARZOZ SANTISTEBAN, Xabier, "Videovigilancia y Derechos Fundamentales: análisis de la constitucionalidad de la Ley Orgánica 4/1997", *REDC* nº 64, 2002;

-"Artículo 8 CEDH. Derecho al respeto de la vida privada y familiar", LASAGABASTER HERRARTE, Iñaki (Dir.), *Convenio Europeo de Derechos Humanos. Comentario Sistemático,* Thomson-Civitas y Eusko Jaurlaritza-Gobierno Vasco, Madrid, 2004.

-"La relevancia del Derecho de la Unión Europea para la Interpretación de los Derechos Fundamentales Constitucionales", *REDC,* nº 74, 2005;

-*Videovigilancia, seguridad ciudadana y Derechos Fundamentales,* Thomson Reuters y Civitas, Cizur Menor, 2010.

ATELA BILBAO Alfonso y GARAY ISASI, Josu, "Ley 41/2002 de Derechos del Paciente. Avances, Deficiencias y Problemática", PÉREZ GONZÁLEZ, Pedro y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre),* Thomson-Civitas, Madrid, 2004.

AYALA MUÑOZ, José María, "Artículos 60 y 61. Prueba", RIVERO GONZÁLEZ, Manuel (Coord.), *Comentarios a la Ley de la Jurisdicción Contencioso-Administrativa de 1998,* Aranzadi, Pamplona, 1999.

AYERA LAZCANO, José María, "Regulación General de la Historia Clínica", *DS*, vol. 11 nº 1, 2003.

BACARAIA MARTRUS, Jordi, "La aplicación de los principios básicos de la normativa sobre protección de datos a los datos médicos", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de protección de Datos de Carácter Personal en el ámbito de la Salud*, APDCat, Madrid, 2006.

BACIGALUPO, Enrique, *Teoría y Práctica del Derecho Penal (Tomo I)*, Marcial Pons, Madrid, 2009.

BALAGUER CALLEJÓN, Francisco, *Derecho Constitucional (vol. II)*, Tecnos, Madrid, 2003.

BALLESTER DÍEZ, F., y VALCÁRCEL RIVERA, Y., "Epidemiología ambiental", VVAA, *Manual de Epidemiología y Salud Pública,* Editorial Médica Panamericana, Madrid, 2008.

BALLESTERO, Fernando, *La Brecha Digital. El Riesgo de Exclusión en la Sociedad de la Información,* Fundesco/Retevisión, Madrid, 2002.

BARATA I MIR, Joan, "Veracidad y Objetividad en el tratamiento de la Información: reflexiones a partir del tratamiento informativo, por parte de la BBC del denominado <<caso nelly>>", *REDC*, nº 69, 2003.

BARCELÓ, Rosa y PÉREZ ASINARI, María Verónica, "Transferencia Internacional de Datos Personales", MARTÍNEZ MARTÍNEZ, Ricard (Coord.) *Protección de Datos. Comentarios al Reglamento de Desarrollo de la LOPD,* Tirant lo Blanch, Valencia, 2009.

BARNÉS, Javier, "Introducción al Principio de Proporcionalidad en el Derecho Comparado Comunitario", *RAP*, nº 135, 1994;

-"Una Reflexión Introductoria sobre el Derecho Administrativo y la Administración Pública de la Sociedad de la Información y el Conocimiento"*, RAAP*, nº 40, 2000.

BARRIUSO RUIZ, Carlos, *Administración Electrónica,* Dykinson, Madrid, 2007.

BASSOLS COMA, Martín, "Los Principios del Estado de Derecho y su Aplicación a la Administración en la Constitución", *RAP,* nº 87, 1978.

BAYO DELGADO, Joaquín, "Los artículos 22, 23.1 y 24.1 LOPD", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

BAZÁN ÁLVAREZ, Antonio, "El consentimiento en las actividades docentes", LEÓN SANZ, Pilar (ed.), *La implantación de los derechos del paciente,* EUNSA, Barañaín, 2004.

BELTRÁN, Josep Mª, COLLAZO, Eliseo, GERVÁS, Juan, GONZÁLEZ SALINAS, Pedro, GRACIA, Diego, JÚDEZ Javier, RODRÍGUEZ SENDÍN Juan José, RUBÍ Jesús, SÁNCHEZ Miguel, *Guías de Ética en la Práctica Médica: Intimidad, Confidencialidad y Secreto,* Fundación Ciencias de la Salud, Madrid, 2005.

BELLIDO PENADES, Rafael, "Las diligencias preliminares", GIMENO SENDRA, Vicente (Dir.), *Proceso Civil Práctico*, La Ley, Madrid, 2002.

BELLO JANEIRO, Domingo, *Responsabilidad civil del médico y responsabilidad patrimonial de la Administración sanitaria*, Asisa, Madrid, 2009.

BENAC URROZ, Mariano, "La Problemática del Menor Maduro en la Obtención del Consentimiento Informado", GONZÁLEZ SALINAS, Pedro y LIZARRAGA BONELLI, Emilio

(Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

BENITO, Fernando, "España", VVAA, *Protección de la Salud. IV Informe sobre Derechos Humanos*, Trama, Madrid, 2006.

BERNAL PULIDO, Carlos, *El Principio de Proporcionalidad y los Derechos Fundamentales,* Centro de Estudios Políticos y Constitucionales, Madrid, 2007.

BILBAO UBILLOS, Juan Mª, *La eficacia de los Derechos Fundamentales frente a particulares. Análisis de la jurisprudencia del Tribunal Constitucional del Tribunal Constitucional*, CEPC, Madrid, 1997.

BLANQUER, David, *Introducción al Derecho Administrativo*, Tirant lo Blanch, Valencia, 1998.

BLAS ORBAN, Carmen, *El equilibrio en la relación médico paciente*, Bosch, Barcelona, 2006.

BLEDA, J. Mª; De SEBASTIÁN, L. y ROVIROSA, J., "Estudios sobre la Actitud y Opinión del Personal Sanitario sobre la Implantación de la Telemedicina en el Complejo Hospitalario y Universitario de Albacete"*, Gestión Hospitalaria*, vol. 10, nº 1, 1 enero 1999, http://www.doyma.es/.

BORDES SOLANAS, Montserrat, "Investigación médica y genética y protección de datos", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el ámbito de la salud*, Marcial Pons y APDCat, Madrid, 2006.

BORRAJO DACRUZ, Efrén, "Comentario al artículo 43 de la Constitución", ALZAGA VILLAMIL, Oscar (Dir.), *Comentarios a la Constitución Española de 1978 (Tomo IV)*, Cortes Generales. Editoriales de Derecho Reunidas., Madrid, 1996.

BRAGE CAMAZANO, Joaquín, *Los Límites a los Derechos Fundamentales,* Dykinson, Madrid, 2004;

-"Aproximación a una Teoría General de los Derechos Fundamentales en el Convenio Europeo de Derechos Humanos", *REDC,* nº 74, 2005.

BROGGI TRIAS, Marc Antoni, "Algunos problemas de la información clínica en la puesta en práctica del consentimiento informado escrito", *EDJ*, nº 7, vol. 1, 1997.

BUISÁN GARCÍA, Nieves, "Movimiento Internacional de Datos", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2008;

-"Comunicación de datos", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008.

-“Acceso a los Datos por Cuenta de Terceros”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008;

-“Derechos de las personas”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2008

CALVO SÁNCHEZ, Luis, *Régimen jurídico de los Colegios Profesionales*, Civitas, Madrid, 1998.

CAMPUZANO TOMÉ, Herminia, “Las redes sociales digitales: concepto, clases y problemática jurídica que plantean en los albores del siglo XXI”, *AC* nº 1, 2011.

CANALES GIL, Álvaro, “Derecho de información en la recogida de datos”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

CANO CAMPOS, Tomás, “Sanciones administrativas”, *RGDA,* nº 16, 2007, http://www.iustel.com

CANO CERVIÑO, Cesar, FERRER RIPOLLES, Carmen, SIGNES ANDREU, Juan Miguel y TOLOSA FUERTES, Laura, “El Lenguaje: Elemento Clave para la Integración de los Sistemas de Información Sanitarios”, Ponencia presentada en el VI Congreso de Informática y Salud, Infors@lud-net 2003, 2-4 abril 2003, http://www.seis.es/.

CANTERO MARTÍNEZ, Josefa, *La Autonomía del Paciente: del Consentimiento Informado al Testamento Vital*, Bomarzo, Albacete, 2005.

CANTERO RIVAS, Roberto, “La Historia Clínica en el Proceso: su aportación por los pacientes”, FERNÁNDEZ HIERRO, José Manuel (Coord.), *La Historia Clínica*, Comares, Granada, 2002.

-“La Historia Clínica: propiedad y acceso”, LEÓN SANZ, Pilar (ed.), *La implantación de los derechos del paciente,* EUNSA, Barañaín, 2004;

-“El contenido de la historia clínica: contenido mínimo y reserva profesional del médico. La petición de historia clínica por un órgano judicial: motivación y supuestos. La eventual negativa médica a la entrega de la historia clínica”, VVAA, *El Juez Civil ante la investigación biomédica,* Cuadernos de Derecho Judicial, Madrid, 2004;

-“La historia clínica: naturaleza y régimen jurídico”, VVAA, *El Derecho a la protección de datos en la historia clínica y la receta electrónica,* Aranzadi y Thomson Reuters, Cizur Menor, 2009.

CARBALLO ARMAS, Pedro, *El Defensor del Pueblo. El Ombudsman en España y en el Derecho Comparado,* Tecnos, Madrid, 2003.

CARDONA RUBERT, Mª Belén, *Informática y Contrato de Trabajo,* Tirant lo Blanch, Valencia, 1999;

-"Derechos de acceso, rectificación, cancelación y oposición en el nuevo reglamento de desarrollo de la LOPD", MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Protección de Datos. Comentarios al reglamento de desarrollo de la LOPD*, Tiranto lo Blanch, Valencia, 2009.

CARMONA SALGADO, Concepción, *Libertad de Expresión e Información y sus Límites*, Edersa, Madrid, 1991.

CARNICERO, J y VÁZQUEZ, J. M., "La Identificación, un Requisito Previo a la Historia de Salud Electrónica"*,* VVAA, *Informe SEIS. De la Historia Clínica a la Historia de Salud Electrónica,* 18/12/2003, http://www.seis.es/.

CARNICERO GIMÉNEZ DE AZCÁRATE, Javier, "La historia clínica informatizada", LEÓN SANZ, Pilar (ed.), *La implantación de los derechos del paciente,* EUNSA, Barañaín, 2004.

CARRASCOSA-LÓPEZ, Valentín, "La LORTAD una Necesidad en el Panorama Legislativo Español*", Iy D*, nº 6-7, UNED, 1994;

-"La Regulación Jurídica del Fenómeno Informático", *IyD*, nº 19-22. UNED, 1998.

CARRETERO PÉREZ, Adolfo y CARRETERO SÁNCHEZ, Adolfo, *Derecho Administrativo Sancionador*, Revista de Derecho Privado, Madrid, 1992.

CARRILLO, Marc, "Derecho a la información y la veracidad informativa", *REDC,* nº 23, 1988.

CARRILLO SALCEDO, Juan Antonio, *El Convenio Europeo de Derechos Humanos*, Tecnos, Madrid, 2003.

CARRO VERNÁNDEZ-VALMAYOR, José Luis, "Sobre los Conceptos de Orden Público, Seguridad Ciudadana y Seguridad Pública", *RVAP,* nº 27, 1990.

CASADO CADARSO, María Teresa y VILA MUNTAL, María Angels, "Los ficheros de las Fuerzas y Cuerpos de Seguridad", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

CASADO CASADO, Lucía, "El Derecho de acceso a la información ambiental a través de la jurisprudencia", *RAP,* nº 178, 2009.

CASARES, Miguel, "Es muy difícil salvaguardar la confidencialidad en los centros", *Diario Médico* 20 de octubre de 2004.

CASTELLANO ARROYO, María, "Problemática de la historia clínica", *Actas del Seminario Conjunto sobre <<Información y Documentación Clínica>>,* Consejo General del Poder Judicial y Ministerio de Sanidad y Consumo, Madrid, 1997.

CASTELLANOS, Pedro Luis, "Los Modelos Explicativos del Proceso Salud-Enfermedad: los Determinantes Sociales", en VVAA, *La Salud Pública*, McGraw Hill, Madrid, 1998.

CASTELLS ARTECHE, José Manuel, "El Derecho de Acceso a la documentación de la Administración pública", *RVAP,* nº 10, 1984;

-"Aproximación a la Problemática de la Informática y la Administración Pública", VVAA, *Jornadas Internacionales sobre Informática y Administración Pública,* IVAP-HAEE, Oñati,1986;

-"Derecho a la Privacidad y Procesos Informáticos: análisis de la Ley Orgánica 5/1992, de 29 de octubre (LORTAD)", *RVAP*, nº 39, 1994;

-"El Tratamiento Jurídico de los Documentos y Registros Sanitarios Informatizados y no Informatizados", ponencia presentada en el seminario conjunto sobre información y documentación clínica, Madrid, 22 y 23 de septiembre 1997, *EDJ,* nº 7 vol. II, 1997.

CASTELLS, Manuel, *La Ciudad Informacional. Tecnologías de la Información, Reestructuración Económica y el Proceso Urbano-Regional,* Alianza, Madrid, 1995;

-*La era de la Información: Economía, Sociedad y Cultura* (volúmenes I, II y III), Alianza, Madrid, 1997.

CATALÁ i BAS, Alexandre H., *Libertad de Expresión e Información. La jurisprudencia del TEDH y su recepción por el Tribunal Constitucional*, Revista General de Derecho, Valencia, 2001.

CAZURRO BARAHONDA, Víctor, "Objeto y naturaleza de los códigos tipo", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

CERRILLO i MARTÍNEZ, Agustí, *Administración electrónica,* Thomson-Aranzadi, Cizur Menor, 2007;

-"Comunicación de datos entre administraciones públicas", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

CEVALLOS ALONSO, C., ARTAL CORTÉS, A., CORDOBA DIAZ DE LASPRA, E. y GARCÍA CAMPAYO, J, "Ética y Derecho del paciente en la toma de decisión: principio de autonomía", *Gestión Hospitalaria*, vol. 13, nº 4, 2002, en http://www.doyma.es/.

CIDONCHA, Antonio, *La libertad de empresa,* Thomson-Civitas e Instituto de Estudios Económicos, Cizur Menor, 2006.

CIERCO SEIRA, César, *Administración Pública y Salud Colectiva. El marco jurídico de la protección frente a las epidemias y otros riesgos sanitarios*, Comares, Granada, 2006;

-"Algunas reflexiones sobre la simplificación de los procedimientos administrativos a la luz de los avances de la Administración Electrónica", *RGDA,* nº 18, 2008. En http://www.iustel.com

COBEÑA FERNÁNDEZ, José Antonio, "Evolución de los Sistemas de Información en las Comunidades Autónomas"*, IyS*, nº 15, marzo-abril, 1998, http://www.seis.es/.

COBREROS MENDAZONA, Eduardo, *Los Tratamientos Sanitarios Obligatorios y el Derecho a la Salud (Estudio sistemático de los ordenamientos Italiano y Español*), HAEE-IVAP, Oñati, 1988.

CODÓN HERRERA, Alfonso, "La historia clínica: concepto, normativa, titularidad y jurisprudencia", GONZÁLEZ SALINAS, Pedro y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

COLLADO GARCÍA-LAJARA, Enrique, *Protección de Datos de Carácter Personal. Legislación, Comentarios, Concordancias y Jurisprudencia,* Comares, Granada, 2000.

CONDE ORTIZ, Concepción, *La Protección de Datos Personales. Un derecho autónomo con base en los conceptos de intimidad y privacidad*, Dykinson, Madrid, 2005.

CORCHETE MARTÍN, María José, *El Defensor del Pueblo y la protección de los derechos,* Universidad de Salamanca, Salamanca, 2001.

CORDOBÉS, Antonio, "Informática. Receta Electrónica (I). Proyecto PISTA y Repercusiones Sobre la Oficina de Farmacia", *Offarm*, vol. 21, nº 8, 1 septiembre 2001, http://www.doyma.es/.

-"Informática. Receta Electrónica (II). Proyectos de las Comunidades Autónomas", *Offarm*, vol. 21, nº10, noviembre 2002, http://www.doyma.es/.

CORREDOIRA Y ALFONSO, Loreto, "Internet (II)", VVAA, *Derecho de la Información,* Ariel, Barcelona, 2003.

CORTÉS BECHIARELLI, Emilio, *El Secreto Profesional del Abogado y del Procurador y su Proyección Penal,* Marcial Pons, Madrid, 1998.

COSCULLUELA MONTANER, Luis, *Manual de Derecho Administrativo (Tomo I)*, Thomson-Civitas, Cizur Menor, 2006 (decimoséptima edición).

COTINO HUESO, Lorenzo, "Derechos del Ciudadano", GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián (Coords.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*", Thomson-Civitas, Cizur Menor, 2008.

COUDERT, Fanny, "Tratamiento de datos especialmente protegidos", ALMUZARA ALMAIDA, Cristina (Coord.), *Estudio práctico sobre la protección de datos de carácter personal,* Lex Nova, Valladolid, 2007;

-"Ejercicio de Derechos", ALMUZARA ALMAIDA, Cristina (Coord.), *Estudio práctico sobre la protección de datos de carácter personal*, Lex Nova, Valladolid, 2007;

-“Transferencias Internacionales de Datos”, ALMUZARA ALMAIDA, Cristina (Coord.), *Estudio Práctico sobre la Protección de Datos de Carácter Personal*, Lex Nova, Valladolid, 2007.

COUSIDO GONZÁLEZ, María Pilar, “El derecho de la información en España”, RODRÍGUEZ PARDO, Julián (Coord.), *Derecho de la Información. Una perspectiva comparada de España e Iberoamérica,* Dykinson, Madrid, 2007.

CRESPO del ARCO, José, “Aplicaciones Médicas de Trabajo Colaborativo en Internet”*,* Comunicación presentada en las primeras Jornadas Nacionales de Internet en Salud, Infors@lud-net 98, 24-27 marzo 1998, http://www.seis.es/.

CRESPO, P; MALDONADO, J.A.; ROBLES, M y CHAVARRÍA, M, “Tecnologías de la Información al Servicio de la Historia Clinica Electrónica”*,* VVAA, *Informe SEIS. De la Historia Clínica a la Historia de Salud Electrónica,* 18/12/2003, http://www.seis.es/.

CRIADO DEL RÍO, María Teresa, *Aspectos medico-legales de la Historia Clínica,* Colex, Madrid, 1999.

CRIADO GRANDE, Juan Ignacio y RAMILO ARAUJO, Mari Carmen, “eAdministración, ¿un reto o una nueva moda? Problemas y Pespectivas de Futuro en torno a Internet y las Tecnologías de la Información y las Comunicaciones en las Administraciones Públicas del siglo XXI”*, RVAP*, nº 61, 2001.

CUBERO MARCOS, José Ignacio, “Excepciones al Derecho de Acceso a la Información en materia Medioambiental”, *EDJ*, nº 137, 2007.

-*El principio de Non Bis in Idem* en la Ley Vasca de la Potestad Sancionadora, IVAP-HAEE, Oñati, 2010;

-“Derechos sociales y la libertad de establecimiento y prestación de servicios”, *RVAP,* nº 87-88, 2010.

CUBERO MARCOS, José Ignacio y ABERASTURI GORRIÑO, Unai, “Reflexiones en torno a la protección de los datos personales en las comunicaciones electrónicas”, *RVAP,* nº 78, 2008;

-“Protección de datos personales en las comunicaciones electrónicas: especial referencia a la Ley 25/2007, sobre conservación de datos”, *REDC,* nº 83, mayo-agosto de 2008.

CUERVO, José, “Autodeterminación Informativa”, *Informática jurídica* http://www.informatica-juridica.com/, 1998.

CUETO PÉREZ, Miriam, *Responsabilidad de la Administración en la asistencia sanitaria,* Tirant lo Blanch, Valencia, 1997.

CURREA LUGO, Victor de, *La salud como derecho humano: 15 requisitos y una mirada a las reformas,* Universidad de Deusto, Bilbao, 2005.

CUSTODI, Jordi y GARCÍA, Carlos, "Los Sistemas de Información en el INSALUD"*, Revista de Calidad Asistencial*, vol 17, nº3, 1 mayo 2002, http://doyma.es/.

CHAMORRO BERNAL, Francisco, *La Tutela Judicial Efectiva. Derechos y Garantías procesales derivados del artículo 24.1 de la Constitución*, BOSCH, Barcelona, 1994.

CHAVELI DONET, Eduard, "El Estatuto del Encargado del Tratamiento", MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Protección de Datos. Comentarios al Reglamento de Desarrollo de la LOPD,* Tirant lo Blanch, Valencia, 2009.

CHINCHILLA MARÍN, Carmen, *La Desviación de Poder*, Civitas, Madrid, 1999.

CHUECA RODRÍGUEZ, Ricardo, "El Marco Constitucional del Final de la Propia Vida", *REDC*, nº 85, 2009.

DAVARA RODRÍGUEZ, Miguel Angel, *De las Autopistas de la Información a la Sociedad Virtual,* Aranzadi, Pamplona, 1996;

-*La Protección de Datos en Europa, Principios, Derechos y Procedimiento,* Asnef Equifax, Madrid, 1998;

-"Hacia un nuevo modelo de Derecho"*,* http://www.iee.es/;

-"Los Datos Sanitarios se tratarán sin contar con los Pacientes", *Diariomedico* 14 de febrero del 2000, en http://www.diariomedico.com/;

-*Manual de Derecho Informático* (5ª edición), Aranzadi, Pamplona, 2003;

-*Manual de Derecho Informático* (7ª edición), Aranzadi, Pamplona, 2005;

- *Guía Práctica de Protección de Datos para Ayuntamientos,* La Ley y El Consultor de los Ayuntamientos y de los Juzgados, Móstoles, 2006;

- En APDCM, *Estudios sobre Administraciones Públicas y Protección de Datos Personales (I Encuentro entre Agencias Autonómicas de Protección de Datos Personales)*, Thomson-Civitas y APDCM, Madrid, 2006;

-"La Transferencia Internacional de Datos", *REPD,* nº 1, 2006;

-"El concepto de fichero en la normativa sobre protección de datos", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*", Civitas y Thomson-Reuters, Cizur Menor, 2010;

-*Acceso electrónico de los ciudadanos a los servicios públicos,* La Ley, Madrid, 2010.

DE AHUMADA RAMOS, Francisco Javier, *La Responsabilidad Patrimonial de las Administraciones Públicas. Elementos Estructurales: Lesión de Derechos y Nexo Causal entre la Lesión y el Funcionamiento de los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 2004.

DE ANGEL YAGÜEZ, Ricardo, "Problemática de la Historia Clínica", *EDJ*, nº 7, vol. 1, 1997.

De ASÍS ROIG, Agustín, "Documento Electrónico en la Administración Pública", en GALLARDO ORTIZ, M. A. (Dir.), *Ámbito Jurídico de las Tecnologías de la Información,* Cuadernos de Derecho Judicial, CGPJ, XI, Madrid, 1996.

DE LA MATA BARRANCO, Norberto J., *El Principio de Proporcionalidad Penal*, Tirant lo Blanch, Valencia, 2007.

DE LA OLIVA SANTOS, Andrés, "Sección 7ª", VVAA, *Comentarios a la Ley de Enjuiciamiento Civil*, Civitas, Madrid, 2001.

DE LA VEGA-HAZAS RAMÍREZ, Julio, "Autonomía, dos concepciones éticas", *Revista de Filosofía*, nº 23, 2000.

DEL CASTILLO VÁZQUEZ, Isabel-Cecilia, *Protección de Datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Thomson-Civitas y APDCM, Cizur Menor, 2007.

DELGADO GARCÍA, Ana Mª y OLIVER CUELLO, Rafale (Coordinadores), *Administración Electrónica Tributaria,* BOSCH, Barcelona, 2009.

DELGADO RODRÍGUEZ, M. y LLORCA DÍAZ, J., "Concepto de Salud. El continuo salud-enfermedad. Historia natural de la enfermedad. Determinantes de la salud", VVAA, *Manual de Epidemiología y Salud Pública*, Editorial Médica Panamericana, Madrid, 2008.

DE LORENZO Y MONTERO, Lorenzo, *Derechos y Obligaciones de los Pacientes. Análisis de la Ley 41/2002, de 14 de noviembre, básica reguladora de Autonomía de los Pacientes y de los Derechos de Información y Documentación Clínica*, Colex, Madrid, 2003;

-*Protección de Datos Personales en el Derecho Sanitario*, Colex, Madrid, 2009.

DE LORENZO Y MONTERO, Ricardo y SÁNCHEZ CARO, Javier, "Consentimiento Informado", en GÓMEZ Y DÍAZ CASTROVERDE, José (Dir.), *Lecciones de Derecho Sanitario*, Universidade da Coruña, A Coruña, 1999.

DE LORENZO Y MONTERO, Ricardo y ESCUDERO GONZÁLEZ, Marta, "El derecho de acceso a la historia clínica y la seguridad del paciente", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

Del PESO NAVARRO, Emilio, "Impugnación de valoraciones: ¿un error más?", en http://www.iee.es;

-*Ley de Protección de Datos. La nueva LORTAD,* Díaz de Santos, Madrid, 2000;

-"Principales Diferencias entre la Nueva Ley de Protección de Datos y la LORTAD", *AIA,* nº 34, enero 2000;

-*Manual de Outsourcing Informático. Análisis y contratación,* Diaz de Santos e IEE, Madrid , 2003;

-*Qué Pasa con Nuestros Datos Médicos,* http://www.iee.es/.

DEL PESO NAVARRO, Emilio y RAMOS GONZÁLEZ, Miguel A., *La Seguridad de los Datos de Carácter Personal,* Díaz de Santos, Madrid, 2002.

Del POZO GUERRERO, Francisco y GÓMEZ AGUILERA, Enrique J., "Telemedicina: una Visión del Pasado y del Futuro"*, Todo Hospital*, nº 170, Julio-Agosto 2001.

DEL SAZ, Silvia, *Los Colegios Profesionales,* Marcial Pons, Madrid, 1996.

DE MIGUEL CASTAÑO, Adoración, "Libertad de Información y Derecho a la Intimidad: Medios para garantizarlos. Incidencia en el Ámbito de la Estadística"*, RFDUC*, nº12, 1986.

De MIGUEL SÁNCHEZ, Noelia, *Secreto Médico, Confidencialidad e Información Sanitaria,* Marcial Pons, Madrid, 2003;

-"Intimidad e Historia Clínica en la Nueva Ley 41/2002, de 14 de noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica", *REDA* nº 117, 2003;

-*Tratamiento de Datos Personales en el Ámbito Sanitario: Intimidad <<versus>> Interés Público,* Tirant lo Blanch, Valencia, 2004;

-"Investigación y Protección de Datos de Carácter Personal: una aproximación a la Ley 14/2007, de 3 de julio, de investigación biomédica", *REPD,* nº 1, 2006;

- "Datos de carácter personal relativos a la salud: una obligada remisión a la normativa del sector sanitario", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

DENNINGER, Erhard, "El Derecho a la Autodeterminación Informativa", VVAA, *Problemas Actuales de la Documentación y la Informática Jurídica (actas del coloquio internacional celebrado en la universidad de Sevilla el 5-6 de marzo de 1986)*, Tecnos, Madrid, 1997.

DE OTTO, Ignacio, "La Regulación del Ejercicio de los Derechos y Libertades. La Garantía de su Contenido Esencial en el artículo 53.1 de la Constitución", MARTÍN-RETORTILLO Lorenzo y DE OTTO y PARDO Ignacio, *Derechos Fundamentales y Constitución*, Civitas, Madrid, 1988;

DE PALACIO VALLE-LERSUNDI, “Artículo 19”, ROVIRA VIÑÁS, Antonio (Dir.), *Comentarios a la Ley Orgánica del Defensor del Pueblo*, Aranzadi, Cizur Menor, 2002.

DÍAZ MÉNDEZ, Nicolás, “La Historia Clínica desde el punto de vista legal”, CALCEDO ORDÓÑEZ, Alfredo, (ed.), *Secreto Médico y Protección de Datos Sanitarios en la práctica Psiquiátrica,* Editorial Médica Panamericana, Madrid, 2000;

-“Historia Clínica. Titularidad, acceso, uso y conservación”, VVAA, *El Juez Civil ante la Investigación Biomédica*, Cuadernos de Derecho Judicial, Madrid, 2004.

DÍAZ PINTOS, Guillermo, “El Consentimiento: ¿una Garantía de la Autonomía Moral del Paciente o un Expediente para Eximir de la Responsabilidad?”, *DS*. vol. 6, nº 1, 1998.

DÍAZ REVORIO, Francisco Javier, “Derecho de la información en la recogida de datos: una perspectiva constitucional”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cisura Menor, 2010.

DIETRICH PLAZA, Cristina, “El Tratado de Prüm en el marco de la regulación de la protección de datos personales en la Unión Europea”, *RDCE* nº 7, 2007.

DÍEZ PICAZO, Luis María, *Sistema de Derechos Fundamentales,* Thomson-Civitas, Madrid, 2005.

DÍEZ-PICAZO GIMÉNEZ, Ignacio, “Artículo 24: Garantías Procesales”, ALZAGA VILLAAMIL, Oscar (Dir.), *Comentarios a la Constitución Española.*(Tomo III), Edersa, 2006, http://www.vlex.com

DOMÍNGUEZ LUELMO, Andrés, *Derecho Sanitario y Responsabilidad Médica. Comentarios a la Ley 41/2002, de 14 de noviembre, sobre derechos del paciente, información y documentación clínica,* Lex Nova, Valladolid, 2007.

DORADO, José Mª y FERNÁNDEZ-HERRERA, Jesús, “La Protección de Datos en la práctica privada”, *Actas Dermo-Sifiliográficas,* vol. 97, nº 1, 2006.

DORAL, José Antonio, *El Contrato como Fuente de Obligaciones,* Eunate, Pamplona, 1993.

DORMIDO BENCOMO, Sebastián, “Tecnologías de la Información: Reflexiones sobre el Impacto Social y Humanístico”*, IyD*, nº 19-22, UNED, 1998.

DRUMMOND, Victor, *Internet, Privacidad y Datos Personales,* Reus, Madrid, 2004.

ECHEVARRÍA, Javier, “Ética y Derechos Humanos en la Sociedad de la Información”*,* en VVAA, *La Tecnología de la Información y sus Desafíos,* España Nuevo Milenio, Madrid, 2002.

EGUSQUIZA BALMASEDA, Mª Ángeles, *Protección de Salud: Intimidad y Salud,* Aranzadi y Thomson-Reuters, Cizur Menor, 2009.

ELGUERO MERINO, José María, “Artículo 106”, REGLERO CAMPOS, L. Fernando (Coord.), *Ley de Contrato de Seguro*, Thomson-Aranzadi, Cizru Menor, 2007.

ELIAS BATURONES, Julio José, “La Regulación de los Datos Sensibles en la Directiva 95/46/CE”, VVAA, *IyD,* nº 23-26, UNED, 1998..

EMBID IRUJO, *El Ciudadano y la Administración*, MAP, Madrid, 1994;

-*El Derecho a un Medio Ambiente adecuado*, Iustel, Madrid, 2008.

ENÉRIZ OLAECHEA, Francisco Javier, *La Protección de los Derechos Fundamentales y las Libertades Públicas en la Constitución Espaola,* Universidad Pública de Navarra, Pamplona, 2007.

ESCARRABIL, J., “La Atención Domiciliaria como Alternativa a la Hospitalización Convencional”*, Atención Primaria*, vol. 30, nº5, 30 septiembre 2002, http://www.doyma.es/.

ESCOBAR DE LA SERNA, Luis, *Derecho de la información,* Dykinson, Madrid, 2004.

ESCOLAR CASTELLÓN, Fernando, “La Inferencia de un Sistema de Información Sanitaria basada en la Historia de Salud Electrónica”*,* VVAA, *Informe SEIS. De la Historia Clínica a la Historia de Salud Electrónica,* 18/12/2003, http://www.seis.es/.

ESCOLAR CASTELLÓN, Fernando; IRABURU ELIZONDO, Margarita y MANSO MOSNTES, Eelena, “Modelos de Historia de Salud Electrónica”*,* VVAA, *Informe SEIS. De la Historia Clínica a la Historia de Salud Electrónica,* 18/12/2003, http://www.seis.es/.

ESCRIBANO COLLADO, Pedro, *El Derecho a la Salud*, Cuadernos del Instituto García Oviedo, Sevilla, 1976.

ESPARZA LEIBAR, Iñaki y ETXEBARRIA GURIDI, José Francisco, “Comentario al artículo 6”, LASAGABASTER HERRARTE, Iñaki (Dir.), *Convenio Europeo de Derechos Humanos. Comentario Sistemático*, Civitas y Thomson-Reuters, Cizur Menor, 2009.

ESTADELLA YUSTE, Olga, *La Protección de la Intimidad frente a la Transmisión Internacional de Datos Personales,* Tecnos, Madrid, 1995.

ESTEBAN, M., “Las Notas Personales al margen de la Historia Clínica no se pueden cancelar”, *Diariomedico.com*, 7 de marzo de 2002, en http://www,diariomedico.com

ESTIVAL ALONSO, Luis “El Derecho de Rectificación como Garantía de la veracidad informativa. Aspectos procesales”, *Diario La Ley* nº 6624, 2007.

ETXEBARRIA GURIDI, José Francisco, *La Protección de los Datos de Carácter Personal en el Ámbito de la Investigación Penal*, APD, Madrid, 1998;

- *Las Intervenciones Corporales: Su Práctica y Valoración como Prueba en el Proceso Penal*¸Trivium, Madrid, 1999;

- *Los Análisis de ADN y su Aplicación al Proceso Penal,* Comares, Granada, 2000;

- "Los análisis de ADN en la Ley de Enjuiciamiento Criminal (Reformada por la Ley Orgánica 15/2003, de 25 de noviembre", *La Ley Penal,* nº 4, 2004, http://revista-laleypenal.laley.es/;

- "La LO 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN", *Diario la Ley,* nº 6901, 2008.

FALAGÁN, J.A. y NOGUEIRA, J., "La Información Clínica y de Salud"*,* VVAA, *Informe SEIS. De la Historia Clínica a la Historia de Salud Electrónica,* 18/12/2003, http://www.seis.es/.

FANLO LORAS, Antonio, *El debate sobre colegios profesionales y cámaras oficiales,* Civitas, Madrid, 1992.

-"Encuadre Histórico y Constitucional. Naturaleza y Fines. La Autonomía Colegial", MARTÍN-RETORTILLO BAQUER, Lorenzo (Coord.), *Los Colegios Profesionales a la luz de la Constitución,* Civitas, Madrid, 1996.

FARRÉ TOUS, Santiago, "El encargado del tratamiento en el ámbito de las administraciones públicas", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

FATÁS, José Miguel y GARCÍA SANZ, Javier, "Título Primero. Disposiciones Generales", PALOMAR OLMEDA, Alberto (Coord.), *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre)*, Thomson-Civitas, Cizur Menor, 2008.

FERNÁNDEZ-COSTALES MUÑIZ, Javier, "La confidencialidad de los datos relativos a la salud. Derecho a la información del trabajador y acceso de terceros a los resultados de los reconocimientos médicos", *REPD,* nº 4, 2008.

FERNÁNDEZ CHATEIGNER, Vanesa, "La Protección Jurídica del Secreto de las Comunicaciones en Internet"*, Diario La Ley*, nº 5732, 5 marzo 2003, http://laley.net/.

FERNÁNDEZ ESTEBAN, María Luisa, *Nuevas Tecnologías, Internet y Derechos Fundamentales,* Mc Graw Hill, Madrid, 1998.

FERNÁNDEZ GARCÍA, José Arturo, "Comunicación de datos entre administraciones públicas", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008;

-"Ficheros de las Fuerzas y Cuerpos de Seguridad", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008;

-"Artículo 23. Excepciones a los Derechos de acceso, rectificación y cancelación", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2008.

FERNÁNDEZ HIERRO, José Manuel, "Régimen jurídico general de la Historia Clínica", FERNÁNDEZ HIERRO, José Manuel (Coord.), *La Historia Clínica,* Comares, Granada, 2002.

FERNÁNDEZ-LLIMOS, Fernando, "La Receta Electrónica*",* http://www.sefac.org/.

FERNÁNDEZ-LONGORIA, Paula y FERNÁNDEZ-SAMANIEGO, Javier, "Transferencias internacionales de datos personales", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

FERNÁNDEZ LÓPEZ, Juan Manuel, "El Derecho Fundamental a la Protección de los Datos Personales. Obligaciones que derivan para el Personal Sanitario*", DS*, número extraordinario XI Congreso Derecho y Salud, vol.II, 2003;

-"El Consentimiento del Interesado para el Tratamiento de sus Datos Personales", *en Datospersonales.org, Revista de la APDCM,* nº 3, 10 de julio de 2003, en http://www.datospersonales.org/.

-"Algunas reflexiones sobre los aspectos generales que regula el reglamento de desarrollo de la LOPD", *REPD,* nº 3, 2007;

-"Principio de Consentimiento", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

FERNÁNDEZ PASTRANA, José Mª, *El Servicio Público de la Sanidad: el marco constitucion*al, Civitas, Madrid, 1984.

FERNÁNDEZ RAMOS, Severiano, *El Derecho de Acceso a los Documentos Administrativos,* Marcial Pons, Madrid, 1997.

FERNÁNDEZ SALMERÓN, Manuel, *La Protección de Datos Personales en las Administraciones Públicas,* Thomson-Civitas, Madrid, 2003.

FERNÁNDEZ SALMERÓN, Manuel y VALERO TORRIJOS, Julián, "La difusión de información administrativa en Internet y la protección de los datos personales: análisis jurídico de un proceso de armonización", VVAA, *Transparencia administrativa y Protección de Datos Personales. V*

Encuentro entre Agencias Autonómicas de Protección de Datos Personales, Thomson-Civitas y APDCM, Madrid, 2008.

FERNÁNDEZ-SAMANIEGO, Javier y BERENGUER O´SHEA, Pablo, "Recogida de datos en programas radiofónicos: retos desde el punto de vista de protección de datos de carácter personal", *REPD,* nº 3, 2007.

FERRER ROCA, Olga, *La Telemedicina: Situación Actual y Perspectivas,* Fundación Retevisión, Madrid, 2001.

FIGUERUELO BURRIEZA, Ángela, *El Derecho a la Tutela Judicial Efectiva*, Tecnos, Madrid, 1990.

FREIXAS GUTIERREZ, Gabriel, *La Protección de los Datos de Carácter Personal en el Derecho Español,* BOSCH, Barcelona, 2001.

FROSINI, "Problemas Jurídicos de la Información y la Documentación", VVAA, *Problemas Actuales de la Documentación y la Informática Jurídica (Actas del coloquio internacional celebrado en la Universidad de Sevilla 5 y 6 de marzo 1986),* Tecnos, Madrid, 1987;

-"Informática y Administración Pública"*, RAP*, nº 105, 1994;

-"El jurista en la Sociedad Tecnológica"*, Revista Argumentos de Razón Técnica* nº 2, 1999.

GALVÁN RUIZ, Jesús y GARCÍA LÓPEZ, Pedro, *La Administración Electrónica en España,* Ariel, Barcelona, 2007.

GALLARDO CASTILLO, María Jesús, *Los Principios de la Potestad Sancionadora. Teoría y Práctica*, Iustel, Madrid, 2008.

GALLEGO ANABITARTE, Alfredo, "Las relaciones especiales de sujeción y el principio de la legalidad de la administración constitucional", *RAP,* nº 34, 1961.

GAMERO CASADO, Eduardo, "El Derecho Administrativo ante la Era de la Información", GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián (Coords.), *La Ley de Administración Electrónica. Comentario Sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 2008.

GAMERO CASADO y MARTÍNEZ GUTIÉRREZ, *Legislación de Administración electrónica y de protección de datos*, Tecnos, Madrid, 2008.

-"El Derecho Administrativo ante la *Era de la Información*", GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián (Coords.), *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 2008.

GARBERÍ LLOBREGAT, José, *Los Procesos Civiles de Protección del Honor, la Intimidad y la Propia Imagen*, BOSCH, Barcelona, 2007;

-*El Derecho a la Tutela Judicial Efectiva en la Jurisprudencia del Tribunal Constitucional*, BOSCH, Barcelona, 2008.

GARCÍA-BARRERO, M., "Telemedicina en Europa"*, Gestión Hospitalaria*, vol. 11, nº 1, 1 enero 2000, http://www.doyma.es/.

GARCÍA-BERRIO HERNÁNDEZ, Teresa, *Informática y Libertades. La Protección de Datos Personales y su Regulación en Francia y España,* Universidad de Murcia, Murcia, 2003.

GARCÍA de ENTERRÍA, Eduardo, *La Constitución como Norma y el Tribunal Constitucinal*, Thomson-Civitas, Cizur Menor, 2006.

GARCÍA de ENTERRÍA, Eduardo y FERNÁNDEZ, Tomás Ramón, *Curso de Derecho Administrativo (I),* (*Décima Edición*), Cívitas, Madrid, 2000.

GARCÍA DEL POYO VIZCAYA, Rafael, "Encargado del tratamiento", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

GARCÍA GARCÍA, A. Mª, "Problemas de salud relacionados con el trabajo. Epidemiología laboral", VVAA, *Manual de epidemiología y salud pública,* Editorial Médica Panamericana, Madrid, 2008.

GARCÍA GIL, Francisco Javier, *El Proceso Contencioso-Administrativo. Conforme a la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa. Comentarios y Jurisprudencia,* Dilex, Madrid, 1998.

GARCÍA GÓMEZ DE MERCADO, Francisco, *Responsabilidad Patrimonial de la Administración. Cuando y Cómo indemniza la Administración. Especial consideración del ámbito urbanístico y de otros sectores específicos de la Administración*, Comares, Granada, 2009.

GARCÍA GÓMEZ, Montserrat, "Sistema de Información Sanitaria sobre salud laboral: SISAL"*, IyS*, nº 39, febrero 2003, http://www.seis.es/.

GARCÍA MACHO, Ricardo, *Reserva de Ley y Potestad Reglamentaria,* Ariel, Barcelona, 1988;

-*Las Relaciones de Especial Sujeción en la Constitución Española*, Tecnos, Madrid, 1992;

-"Derecho de acceso a la información y protección de datos en la sociedad de la información", VVAA, *Derechos Fundamentales y otros estudios. Homenaje al profesor Dr. Lorenzo Martín-Retortillo (Volumen I) ,* Gobierno de Aragón, Cortes de Aragón, El Justicia de Aragón, Caja Inmaculada, Ibercaja y Facultad de Derecho de la Universidad de Zaragoza, Zaragoza, 2008;

-Los Derechos Fundamentales Sociales y el Derecho a una Vivienda como Derechos Funcionales de Libertad", *RCDP,* nº 38, 2009;

-"El derecho a la información, la publicidad y transparencia en las relaciones entre la Administración, el ciudadano y el público", GARCÍA MACHO, Ricardo (ed.), *Derecho administrativo de la información y administración transparente*, Marcial Pons, Madrid-Barcelona-Buenos Aires, 2010.

GARCÍA MESEGUER, Mª. Dolores y MEDRÁN VIOQUE, Rafael, "España: la Protección de las Personas en el Tratamiento de Datos: Principios y Derechos. Breve Comentario de la Transposición de la Directiva 95/46/CE a la Ley Orgánica 15/1999", *REDI,* nº 46 mayo 2002, en http://premium.vlex.com/.

GARCÍA MEXÍA, Pablo, "El Derecho de Internet y sus Implicaciones para la Administración"*, DAD*, nº 265-266, 2003.

GARCÍA ORTEGA, Cesáreo, CÓZAR MURILLO, Victoria, y ALMENARA BARRIOS, José, "La autonomía del paciente y los derechos en materia de información y documentación clínica en el contexto de la Ley 41/2002", *Revista Española de Salud Pública,* nº 4, 2004.

GARCÍA POGGIO, Paz, "Hacia una Nueva Administracion Pública en la Sociedad de la Información"*, AIA*, nº 32, julio 1998.

GARCÍA ROJO, Marcial, "Formación Médica Continuada y Desarrollo Profesional Continuo"*, IyS*, nº 31, junio-julio 2001, http://www.seis.es/.

GARCÍA URETA, Agustín, *La Potestad Inspectora de las Administraciones Públicas*, Marcial Pons, Madrid, 2006.

GARCÍA VILA, Mónica, "Los cacheos: delimitación y clases", *AP*, XIII, tomo 1, 2000.

GARDAIN, Anja-María, "Transferencia de datos personales a países terceros: Reglamentos Corporativos de Carácter Obligatorio, "Nuevos instrumentos jurídicos" Derecho aplicable", *Datospersonales.org,* nº 17, 2005.

GARRIDO FALLA, Fernando, "Comentario al artículo 43", GARRIDO FALLA, Fernando (Dir.), *Comentarios a la Constitución*, Civitas, Madrid, 2001.

GARRIDO GUTIÉRREZ, Pilar, "El Valor Constitucional de los Principios Rectores (Comentario a la STC 222/1992, de 11 de diciembre)", *RVAP* nº 40, 1994.

GARRIGA DOMÍNGUEZ, Ana, *La Protección de Datos Personales en el Derecho Español,* Dykinson, Madrid, 1998;

-*Tratamiento de Datos Personales y Derechos Fundamentales,* Dykinson, Madrid, 2009 (2ª edición).

GARRORENA MORALES, Ángel, *El Estado Español como Estado Social y Democrático de Derecho*, Tecnos, Madrid, 1984.

GAVARA DE CARA, Juan Carlos, *Derechos Fundamentales y Desarrollo Legislativo. La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn*, CEC, Madrid, 1994.

GAY FUENTES, Celeste, *Intimidad y Tratamiento de Datos en las Administraciones Públicas,* Complutense, Madrid, 1995

GIL-ROBLES y GIL DELGADO, Álvaro, "Los derechos de los ciudadanos en el sistema sanitario", *DS* vol. 2 nº 2, 1994.

GIMENO SENDRA, Vicente, "Información Clínica", ponencia presentada en el Seminario Conjunto sobre Información y Documentación Clínica, Madrid 22 y 23 de septiembre 1997, *EDJ,* nº7, vol. I, 1997.

GÓMEZ AMIGO, Luis, *Las Intervenciones Corporales como Diligencias de Investigación Penal*, Thomson-Aranzadi, Cizur Menor, 2003.

GÓMEZ DE ARRIBA, Daniel, *El Consentimiento Informado en Medicina: el Menor Maduro*, 2001, en http//:www.protegemostusdatos.com/.

GÓMEZ ESTEBAN, Rosa, *El Médico como Persona en la relación Médico-Paciente,* Fundamentos, Madrid, 2002.

GÓMEZ JUÁREZ SIDERA, Isidro, "Breve reflexión acerca del derecho a la protección de los datos de carácter personal de los nascituri", *Datospersonales.org* nº 29, 2007, http://www.madrid.org.

GÓMEZ NAVAJAS, Justa, *La Protección de los Datos Personales,* Thomson-Civitas y APDCM, Cizur Menor, 2005.

GÓMEZ PIQUERAS, Cristina, "Anonimización y disociación de datos personales en la investigación: cuestiones a resolver", VVAA, *Protección de datos e investigación médica,* Aranzadi y Thomson-Reuters, Cizur Menor, 2009;

-"La historia clínica. Aspectos conflictivos resueltos por la Agencia Española de Protección de Datos", VVAA, *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica,* Aranzadi y Thomson Reuters, Cizur Menor, 2009.

GÓMEZ-REINO CARNOTA, Enrique, "Las Libertades Públicas en la Constitución", FERNÁNDEZ RODRÍGUEZ, Tomás Ramón (Coord.), *Lecturas sobre la Constitución Española*, UNED, Madrid, 1978.

GÓMEZ RIVERO, Mª del Carmen, *La Protección Penal de los Datos Sanitarios,* Comares, Granada, 2007.

GÓMEZ SÁNCHEZ, Yolanda, *Derechos y Libertades,* Sanz y Torres, Madrid, 2003;

- "Datos de salud como datos especialmente protegidos", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

GÓMEZ TOMILLO, Manuel, "Límites al deber de secreto médico y derecho penal", *RGDP,* nº 12, 2009.

GONZÁLEZ AMUCHÁSTEGUI, Jesús, *Autonomía, Dignidad y Ciudadanía,* Tirant lo Blanch, Valencia, 2004.

GONZÁLEZ BARRIOS, Iván, "Artículo 11", REGLERO CAMPOS, L. Fernando (Coord.), *Ley de Contrato de Seguro*, Thomson-Aranzadi, Cizru Menor, 2007.

GONZÁLEZ BEILFUSS, Markus, *El Principio de Proporcionalidad en la Jurisprudencia del Tribunal Constitucional*, Thomson-Aranzadi, Navarra, 2003.

GONZÁLEZ CUELLAR SERRANO, Nicolás, *Proporcionalidad y Derechos Fundamentales en el Proceso Penal*, Colex, Madrid, 1990.

GONZÁLEZ MÉNDEZ, Amelia, *La protección de datos tributarios y su marco constitucional,* Tirant lo Blanch, Valencia, 2003.

GONZÁLEZ MORENO, Beatriz, *El Estado Social. Naturaleza Jurídica y Estructura de los Derechos Sociales*, Civitas, Madrid, 2002;

-"La Ley Orgánica de Protección de Datos y los Libros de Bautismo", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

GONZÁLEZ MURUA, Ana Rosa, "Comentario a la STC 254/1993, de 20 de julio. Algunas Reflexiones en torno al artículo 18.4 de la Constitución y la Protección de Datos Personales", *RVAP,* nº 37, 1993.

GONZÁLEZ NAVARRO, Francisco, "La Relación Jurídica de Disposición de Datos de Carácter Personal", HEREDERO HIGUERAS, Manuel (Coord.) *Derecho a la Intimidad y a la Privacidad y las Administraciones Públicas,* Xunta de Galicia, Santiago de Compostela, 1999.

GONZÁLEZ PÉREZ, Jesús, *Responsabilidad Patrimonial de las Administraciones Públicas*, Civitas, Madrid, 1996.

-Comentarios a la Ley de la Jurisdicción Contencioso Administrativa (Ley 29/1998, de 13 de julio) (Tomo II), Civitas, Madrid, 1998.

GONZÁLEZ RAMALLO, Victor José, VALDIVIESO MARTÍNEZ, Bernardo y RUIZ GARCÍA, Vicente, "Hospitalización a Domicilio"*, Medicina Clínica*, vol. 118, nº 117, 2002, http://www.doyma.es/.

GONZÁLEZ RIVAS, Juan José y ARANGUREN PÉREZ, Ignacio, *Comentarios a la Ley reguladora de la Jurisdicción Contencioso Administrativa 29/1998, de 13 de julio,* Thomson-Civitas, Cizur Menor, 2006.

GONZÁLEZ-TABLAS SASTRE, Rafael, "El Derecho y las Nuevas Tecnologías", *AJR*, nº6-7,2000-2001.

GONZÁLEZ TOBARRA, Pedro y JIMÉNEZ CARBAJO, José Ramón, "El Principio de Legalidad: Los Principios de Reserva de Ley, Irretroactividad y Tipicidad", VVAA, *Manual de derecho administrativo sancionador* (Tomo I), Thomson Reuters-Aranzadi, Cizur Menor, 2009.

GOÑI SEÍN, José Luis, *La Videovigilancia Empresarial y la Protección de Datos Personales*, Thomson-Civitas y APDCM, Cizur Menor, 2007.

GOST GARDE, Javier, "Gestión Sanitaria y Tecnologías de la Información"*,* VVAA, *Informe SEIS. Seguridad y Confidencialidad de la información clínica,* 12/12/2000, http://www.seis.es/.

GRACIA GUILLÉN, Diego, "La confidencialidad de los datos clínicos", CALCEDO ORDÓÑEZ, Alfredo (ed.), *Secreto médico y protección de datos sanitarios en la práctica psiquiátrica*, Editorial Médica Panamericana y Lex, Madrid, 2000.

GRACIANO REGALADO, Juan Carlos, "Ficheros de Información sobre Solvencia Patrimonial y Crédito: los Ficheros RAI y ASNEF", *La Ley* nº 2-2005.

GRIMALT SERVERA, Pedro, *La responsabilidad civil en el tratamiento automatizado de datos personales,* Comares, Granada, 1999.

GUERRERO PICÓ, María del Carmen, *El Impacto de Internet en el Derecho Fundamental a la Protección de Datos de Carácter Personal,* Thomson-Civitas y APDCM, Cizur Menor, 2006.

GUERRERO ZAPLANA, José, "El Consentimiento Informado en la Ley de Castilla y León 8/2003, de 8 de abril, sobre Derechos y Deberes de las personas en relación con la Salud", *RJCyL,* nº 1, 2003;

-"Tipos de infracciones", LESMES SERRANO, Carlos, *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008.

GUICHOT, Emilio, "El Nuevo Derecho Europeo de Acceso a la Información Pública", *RAP,* nº 160, 2003;

-*Datos personales y Administración Pública,* Thomson-Civitas y APDCM, Navarra, 2005;

-“Acceso a la información en poder de la Administración y Protección de datos personales”, *RAP,* nº 173, 2007.

-*Publicidad y Privacidad de la Información Administrativa,* Thomson-Civitas y APDCM, Cizur Menor, 2009.

GUTIÉRREZ GUTIÉRREZ, Ignacio, *Criterio de eficacia de los Derechos Fundamentales en las relaciones entre particulares,* Teoría y Realidad Constitucional, nº 3, 1999.

HÄBERLE, Pedro, “El legislador de los Derechos Fundamentales. 5 *”, LÓPEZ PINA, Antonio (Dir.), *La Garantía Constitucional de los Derechos Fundamentales. Alemania, España, Francia e Italia*, Civitas, Madrid, 1991.

HELGUERO SAINZ, José, “Objeto y naturaleza de los códigos tipo”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

HEREDERO HIGUERAS, Manuel, “La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de la Población de 1983”*, DAD*, nº 198, 1983;

-“Ante la Ratificación del Convenio de Protección de Datos del Consejo de Europa”, *DAD*, nº 199, 1983;

-“La Protección de Datos de Salud Informatizados en la LO 5/1992, de 29 de octubre*”, DS*, nº1, vol.2, enero-junio 1994;

-*La Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. Comentario y Textos,* Tecnos, Madrid, 1996;

- *La Directiva Comunitaria de Protección de los Datos de Carácter Personal,* Aranzadi, Pamplona, 1997;

-“La Protección de los Datos de Carácter Personal en el Proyecto de Ley Orgánica de adaptación de la Ley Orgánica 5/1992”, HEREDERO HIGUERAS, Manuel (Coord.) *El Derecho a la Intimidad y a la Privacidad y las administraciones públicas*, Xunta de Galicia, Santiago de Compostela, 1999;

-“La Transmisión Internacional de los Datos de Salud”, RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud,* APDCat y Marcial Pons, Madrid, 2006.

HERNÁNDEZ-AGUADO, I., LUMBRERAS LACARRA, B., GARCÍADE LA HERA, M., “Concepto y Funciones de la Salud Pública”, VVAA, *Manual de Epidemiología y Salud Pública*, Editorial Médica Panamericana, Madrid, 2008.

HERNANDO, Pablo, SEOANE, José Antonio, DE ASÍS, José Francisco, "La Reserva de las Anotaciones Subjetivas: ¿Derecho o Privilegio?", en *Revista de Calidad Asistencial,* vol. 21, nº 1, 2006, en http://www.db.doyma.es/.

HERRAN ORTIZ, Ana Isabel, *La Violación de la Intimidad en la Protección de Datos Personales,* Dykinson, Madrid, 1998;

-"La Protección de Datos Personales en el Marco de la Unión Europea", *REDI* nº 39, 2001, en http://premium.vlex.com/;

-El Derecho a la Intimidad en la Nueva Ley Orgánica de Protección de Datos Personales, Dykinson, Madrid, 2002;

- *El Derecho a la Protección de Datos Personales en la Sociedad de la Información*, Universidad de Deusto, Bilbao, 2003.

HERRANZ RODRÍGUEZ, Gonzalo, "Aspectos Éticos de la Telemedicina", VII Congreso Nacional de Derecho Sanitario, Madrid 19-21 octubre 2000.

HOURS, José Enrique, "Receta Electrónica", *Informática y Salud*, nº 36, mayo 2002, http://www.seis.es/.

IBÁÑEZ FRAILE, Antonio, "Historia Clínica Electrónica", MORO AGUADO, Jesús y TEJEDOR MUÑOZ, Jesús (Coords.), *La Historia Clínica. Contenidos y Requerimientos en las Comunidades Autónomas,* Universidad de Valladolid, Salamanca, 2003.

IBÁÑEZ MÉNDEZ, Inés, "Los Poderes Públicos y la defensa del Medioambiente", *Observatorio medioambiental,* nº 6, 2003.

IBARZABAL, Xabier, "Bioética: tomando decisiones para el final de la vida. Pensando en el principio de autonomía", *Revista Multidisciplinar de Gerontología*, nº 14-3, 2004.

ILLESCAS RUS, Ángel Vicente, *La Prueba Pericial en la Ley 1/2000, de Enjuiciamiento Civil*, Aranzadi, Cizur Menor, 2003.

JACQUEMIN, Herve, "La Telemedicina en Derecho Comparado: Algunos Aspectos Jurídicos", *Diario La Ley*, nº 5795, 4 junio 2003, http://www.laley.net/.

JIMÉNEZ CAMPO, Javier, "Comentario al artículo 53 de la Constitución", ALZAGA VILLAAMIL, Oscar (Dir.), *Comentarios a la Constitución Española de 1978 (Tomo IV)*, Cortes Generales. Editoriales de Derecho Reunidas, Madrid, 1996.

JIMÉNEZ PLAZA, Maria Isabel, *El Derecho de Acceso a la Información Municipal*, Iustel, Madrid, 2006.

JORDANA, Jacint, "Las Administraciones Públicas y la Promoción de la Sociedad de la Información: Opciones Estratégicas y Modalidades de Intervención", *GAPP*, nº 16, 1999.

JORGE BARREIRO, Agustín, “Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”, JORGE BARREIRO, Agustín (Coord.), *Comentarios al Código Penal*, Civitas, Madrid, 1997.

KUKK, Urmas, “Los medios de comunicación y la protección de datos personales”, *Datospersonales.org* nº 30, 2007.

LAFARGA i TRAVER, Joseph Lluis, “Problemas Legales asociados al Tratamiento Informático de la Historia Clínica: la Responsabilidad Médica en el Tratamiento de Datos”, *DS,* vol. 7 nº 2, 1999.

LAMARCA PÉREZ, Carmen, “Autonomía de la Voluntad y Protección Coactiva de la Vida”, *La Ley Penal,* nº 60, 2009, http://revista-laleypenal.laley.es/

LARIOS RICO, David, “La Historia Clínica como conjunto de datos especialmente protegidos”, VVAA, *El derecho a la protección de datos en la historia clínica y la receta electrónica,* Aranzadi y Thomson Reuters, Cizur Menor, 2009.

LARRAZABAL BASAÑEZ, Santiago, *Curso de Derecho Constitucional,* Deusto, Bilbao, 2008.

LASAGABASTER HERRARTE, Iñaki, *Las Relaciones de Sujeción Especial*, IVAP-HAEE y Civitas, Madrid, 1994, p. 61;

-“Introducción”, LASAGABASTER HERRARTE, Iñaki (Dir.), *Convenio Europeo de Derechos Humanos. Comentario Sistemático*, Eusko Jaurlaritza-Gobierno Vasco y Thomson-Civitas, Madrid, 2004;

-“Non bis in idem”, LASAGABASTER HERRARTE, Iñaki (Director), *Ley de Potestad Sancionadora. Comentario Sistemático*, LETE, Bilbao, 2006;

-*Fuentes del Derecho,* LETE, Bilbao, 2007;

-“Notas sobre el derecho administrativo de la información”, GARCÍA MACHO, Ricardo (ed.), *Derecho administrativo de la información y administración transparente*, Marcial Pons, Madrid-Barcelona-Buenos Aires, 2010.

LASAGABASTER HERRARTE, Iñaki, GARCÍA URETA, Agustín y LAZCANO BROTONS, Iñigo, *Derecho Ambiental. Parte General (segunda edición)*, LETE, Bilbao, 2007.

LAZCANO BROTÓNS, Iñigo, “Comentario al artículo 10 del CEDH. Libertad de expresión”, LASAGABASTER HERRARTE, Iñaki (Dir.), *Convenio Europeo de Derechos Humanos. Comentario Sistemático*, Thomson Reuters-Civitas, Cizur Menor, 2009.

LEGALIA, *La Protección de Datos Personales en el Ámbito Sanitario,* Aranzadi, Navarra, 2002.

LEÓN, Gonzalo, “El Papel de la Tecnología como Catalizador del Desarrollo de la Sociedad del Conocimiento”*,* en *La Tecnología de la Información y sus desafíos,* España Nuevo Milenio, Madrid, 2002.

LESMES SERRANO, "Prueba", ARNALDO ALCUBILLA, Enrique y FERNÁNDEZ VALVERDE, Rafael (Dirs.), *Jurisdicción Contencioso-Administrativa (Comentarios a la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa),* El Consultor de los Ayuntamiento y de los Juzgados, Madrid, 1998;

-"Artículo 1. Objeto", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008;

-"Artículo 2. Ámbito de aplicación", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2008;

-"Artículo 3. Definiciones", LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008.

LIZARRAGA BONELLI, Emilio, "La Información y la Obtención del Consentimiento en la nueva Ley 41/2002, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en Materia de Información y Documentación Clínica", GONZÁLEZ SALINAS, Pedro y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

LOPERA MESA, Gloria Patricia, *Principio de Proporcionalidad y Ley Penal,* CEPC, Madrid, 2006, p. 39.

LOPERENA ROTA, Demetrio Ignacio, "La protección de la salud y el medio ambiente adecuado para el desarrollo de la persona en la Constitución", MARTÍN-RETORTILLO BAQUER, Sebastián (Coord.), *Estudios sobre la Constitución Española. Homenaje al Profesor Eduardo García de Enterría (II)*, Civitas, Madrid, 1991.

LÓPEZ, Pau, MOYA, Francesc, MARIMÓN, Santiago y PLANAS, Ignasi, *Protección de Datos de Salud. Criterios y Plan de Seguridad,* Díaz de Santos, Madrid, 2001.

LÓPEZ AGÚNDEZ, José María, "El Respaldo Legal para Tratar Datos de Salud no Exime de Informar", *Diario Médico*, 17 de octubre de 2003, en http://www.diariomedico.com/.

LÓPEZ BENÍTEZ, Mariano, *Naturaleza y presupuestos constitucionales de las relaciones especiales de sujeción,* Civitas, Madrid, 1994.

LÓPEZ CARMONA, Francisco José, "E-Salud, Confidencialidad y Seguridad de la Información en el Ámbito Sanitario", ponencia presentada en el I Encuentro entre Agencias de Protección de Datos, celebrado en Getafe el 24 de noviembre de 2004.

LÓPEZ DEL MORAL ECHEVERRÍA, José Luis, "Impugnación de valoraciones", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

LÓPEZ DOMÍNGUEZ, Orencio, “La Información en los Centros Sanitarios: Situación Actual, Conflictos y Tendencias”, ponencia presentada en el Seminario Conjunto sobre Información y Documentación Clínica, Madrid 22 y 23 de septiembre 1997, *EDJ,* nº 7, vol. II, 1997.

LÓPEZ-ESCOBAR, Esteban, “Comunicación, Participación Ciudadana y Nuevas Tecnologías: una Perspectiva desde la Globalización”*, AJR*, nº 6-7, 2000-2002.

LÓPEZ GARRIDO, Diego, “Aspectos de Inconstitucionalidad de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal”, *RDP*, nº 38, 1994.

LÓPEZ GONZÁLEZ, Ramillo, “Documentaciòn Clínica e Internet –Ventajas y Riesgos”*,* Comunicación presentada en Infors@lud-net 98, 24-27 marzo 1998, http://www.seis.es/.

LÓPEZ GONZÁLEZ, José Luis, *Los Colegios Profesionales como Corporaciones de Derecho Público: un estudio en clave constitucional*, Política y Derecho, Valencia, 2001.

LÓPEZ GUERRA, Luis, ESPÍN, Eduardo, GARCÍA MORILLO, Joaquín, PÉREZ TREMPS, Pablo, SATRUSTEGUI, Miguel, *Derecho Constitucional (vol I)*, Tirant lo Blanch, Valencia, 2002.

LÓPEZ-IBOR MAYOR, Vicente y GARCÍA DELGADO, Sonsoles, “Situación del Derecho Informático en España y en Europa: algunas Consideraciones”*, IyD*, nº 4, UNED, 1994.

LÓPEZ LÓPEZ, Angel M., *La disciplina constitucional de la propiedad privada*, Tecnos, Madrid, 1988.

LÓPEZ MUÑIZ GOÑI, Miguel, “La Ley de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal”, *IyD*, nº 6-7, UNED, 1994.

LÓPEZ ULLA, Juan Manuel, “El consentimiento del afectado en el tratamiento de datos relativos a la salud”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

LORDA, Pablo Simón, *El Consentimiento Informado. La Historia, Teoría y Práctica*, Triacastela, Madrid, 2000.

LOSANO, Mario G., PÉREZ LUÑO, Antonio-Enrique y GUERRERO MATEUS Mª Fernanda, *Libertad Informática y Leyes de Protección de Datos Personales,* CEC, Madrid, 1989.

LOSCERTALES ABRIL, Felicidad y GÓMEZ GARRIDO, Ascensión, *La Comunicación con el Enfermo. Un instrumento al servicio de los profesionales de salud*, Alhulia, Granada, 1999.

LUCAS DURÁN, Manuel, *El Acceso a los Datos en poder de la Administración Tributaria,* Aranzadi, Pamplona, 1997.

LUNA ABELLA, “Artículo 22”, ROVIRA VIÑÁS, Antonio (Dir.), *Comentarios a la Ley Orgánica del Defensor del Pueblo*, Aranzadi, Cizur Menor, 2002.

MARCHENA GÓMEZ, Manuel, "Conocimiento por el interesado de su inclusión en ficheros automatizados sobre solvencia patrimonial", *AJA*, nº 400, 1999.

MAGRO SERVET, Vicente, "La Actuación Policial en los Cacheos y Registros como modalidad de las Intervenciones Corporales en el Proceso Penal", *Diario la Ley,* nº 5357, 2001, http://diariolaley.laley.es/;

-"La delincuencia informática. ¿Quién gobierna en Internet?", *Diario La Ley*, nº 6077, 2004, http://diariolaley.laley.es/

MARIMÓN, Santiago, *La Sanidad en la Sociedad de la Información. Sistemas y Tecnologías de la Información para la Gestión y la Reforma de los Servicios de Salud,* Díaz de Santos, Madrid, 1999.

-"El progreso de los Sistemas de Información Asistenciales", *Revista Calidad Asistencial*, nº 17(3), 2002, en http://www.doyma.es/.

MARÍN PÉREZ, Antonio, "El deber de secreto", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

MARSET CAMPOS, Pedro y SÁEZ GÓMEZ, José Miguel, "La Evolución Histórica de la Salud Pública", VVAA, *Salud Pública*, McGraw Hill, Madrid, 1998.

MARTÍ MONTESINOS, Cristina y PIDEVALL BORRELL, Ignasi, "Accesos a la Historia Clínica, con especial referencia a la Disposición Adicional Tercera de la Ley 41/2002 y al artículo 11.5 referente al Acceso a las Instrucciones Previas", GONZÁLEZ SALINAS, Eduardo y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

MARTÍN CASALLO LÓPEZ, Juan José, "La Regulación del Delito Personal de Salud", en http://www.iee.es/;

-Derechos de Acceso, Rectificación y Cancelación de los Datos Sanitarios en la LOPD, ponencia presentada en el VII Congreso Nacional de Derecho Sanitario, 19-21 octubre 2000, http://www.aeds.org/.

MARTÍN COBISA, Fernando, "Las Nuevas Tecnologías en la Seguridad Social*", IyD*, nº 23-26, UNED, 1998.

MARTÍNEZ AGUADO, Luis Carlos, "Aspectos Éticos de la Historia Clínica", FERNÁNDEZ HIERRO, José Manuel (Coord.), *La Historia Clínica,* Comares, Granada, 2002.

MARTÍNEZ CAMPELLO, Carlos Hernández, "La Ley 41/2002 y la normativa sobre protección y tratamiento de datos de carácter personal relativos a la salud", GONZÁLEZ SALINAS, Pedro y

LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudio sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

MARTÍNEZ FERRIZ, José Luis Jorge, "La operatividad de SITEL: su discutida legalidad dentro de un Estado de derecho que actúa bajo el imperio de la Leu", *Diario La Ley,* nº 7434, 29 junio de 2010, http://diariolaley.laley.es/

MARTÍNEZ HERNÁNDEZ, Juan, *Nociones de Salud Pública*, Diaz de Santos, Madrid, 2003.

MARTÍNEZ HERNÁNDEZ, Juan, ASTIASARÁN ANCHÍA, Iciar y MADRIGAL FRITSCH, Herlinda, *Alimentación y Salud Pública*, McGraw Hill, Aravaca, 2001.

MARTINEZ y HERNÁNDEZ, Eduardo, GARCÍA PERUELLES, Luis Francisco, BARÓN CRESPO, Enrique, *Tratado del Derecho a la Protección de la Salud*, Universidad Complutense de Madrid, Madriod, 2004.

MARTÍNEZ MARTÍNEZ, *Tecnologías de la Información, Policía y Constitución,* Tirant lo Blanch, Valencia, 2001;

-*Una aproximación crítica a la autodeterminación informativa,* Thomson-Civitas y APDCM, Cizur Menor, 2004.

MARTÍNEZ MUÑOZ, Juan Antonio, "Autonomía", *Anuario Jurídico y Económico Escurialense*, nº 40, 2007.

MARTÍNEZ PUJALTE, Antonio Luis, *La Garantía del Contenido Esencial de los Derechos Fundamentales,* CEC, Madrid, 1997.

MARTÍN PALLÍN, José Antonio, "Intimidad, privacidad y protección de datos en la nueva Ley Orgánica de 15/1999, especial referencia a los ficheros policiales", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

MARTÍN PARDO, María, "Los Códigos Tipo: la vía a la autorregulación", *Datospersonales.org,* nº 21, 2005.

MARTÍN PASTOR, José, "Controversia jurisprudencial y avances legislativos sobre la prueba pericial de ADN en el proceso penal (en especial, la base de datos policial sobre identificadores obtenidos a partir del ADN, creada por la Ley Orgánica 10/2007, de 25 de noviembre)", *La Ley penal,* nº 46, 2008, http://revista-laleypenal.laley.es/

MARTÍN REBOLLO, Luis, "La responsabilidad patrimonial de las Administraciones Públicas en España: estado de la cuestión, balance general y reflexión crítica", *DAD*, nº 237-238, 1994.

MARTÍN-RETORTILLO BAQUER, Lorenzo, "El papel de los Colegios en la ordenación de las profesiones y en el control y vigilancia del ejercicio profesional", MARTÍN-RETORTILLO

BAQUER, Lorenzo (Coord.), *Los Colegios Profesionales a la luz de la Constitución,* Civitas, Madrid, 1996.

-"Prólogo", RAMS RAMOS, Leonor, *El Derecho de Acceso a Archivos y Registros Administrativos,* Reus, Madrid, 2008.

MARTÍN SÁNCHEZ, Fernando, "La Congruencia entre la Bioinformática y la Informática médica"*, IyS*, nº 38, noviembre 2002, http://www.seis.es/.

MATA DE ANTONIO, José María, "Problemas Prácticos en torno a la Capacidad Sucesoria del Concepturus", *Revista de Derecho Privado* nº 2003-5, 2003.

MAYER PUJADAS, M.A. y LEIS MACHÍN, A., "El Correo Electrónico en la regulación médico-paciente: uso y recomendaciones generales", *Atención Primaria,* vol. 37, nº 7, 2006, http://www.doyma.es/

MAYORAL BENITO, Raul, "Salud e Internet. Condenados a Entenderse*", Farmacia Profesional*, vol. 15, nº 8, septiembre 2001, http://www.doyma.es/.

MAZÓN RAMOS, Pilar y CARNICERO GIMÉNEZ de AZCÁRATE, Javier, "La Informatización de la Documentación Clínica: Oportunidad de Mejora de la Práctica Clínica y Riesgos para la Seguridad y Confidencialidad"*,* VVAA, *Informe SEIS. Seguridad y Confidencialidad de la Información Clínica,* 12/12/2000, http://www.seis.es/.

MEDINA ALCOZ, Luis, "Responsabilidad Patrimonial de las Administraciones Públicas (II). Elementos. Factores de exoneración", CANO CAMPOS, Tomás (Coord.), *Lecciones y materiales para el estudio del Derecho Administrativo (Tomo IV). Las Garantías de los Ciudadanos y el Control de las Administraciones Públicas,* Iustel, Madrid, 2009.

MEDINA GUERRERO, Manuel, *La Vinculación Negativa del Legislador a los Derechos Fundamentales,* Mc Graw-Hill, Madrid, 1996;

-"Artículo 1", REQUEJO PAGÉS, Juan Luis (Coord.), *Comentarios a la Ley Orgánica del Tribunal Constitucional*, Tribunal Constitucional y BOE, Madrid, 2001;

-*La Protección Constitucional de la Intimidad frente a los Medios de Comunicación*, Tirant lo Blanch, Valencia, 2005.

MEDRANO ALBÉNIZ, Juan, "El secreto médico en perspectiva histórica", CALCEDO ORDÓÑEZ, Alfredo (ed.), *Secreto Médico y Protección de Datos Sanitarios en la práctica Psiquiátrica,* Editorial Médica Panamericana, Madrid, 2000.

MEGÍAS QUIRÓS, José Justo, "Ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas: intimidad, vida privada y protección de datos", TRONCOSO REIGADA, Antonio, (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

MÉJICA GARCÍA, Juan, *El Enfermo Transparente. Futuro Jurídico de la Historia Clinica Electrónica,* Edisofer, Madrid, 2002.

MÉJICA, Juan y DÍEZ José Ramón, "Hacia un Estatuto Jurídico Desarrollado de la Historia Clínica", *Diario La Ley* nº 5638, 22 de octubre de 2002, en http://www.laley.net/;

-*El Estatuto del Paciente. A través de la nueva legislación sanitaria estatal*, Thomson-Civitas, Cizur Menor, 2006.

MÉNDEZ RODRÍGUEZ, Eva María, "Globalización de la Información", en CARIDAD SEBASTIÁN, Mercedes (Coordinadora), *La Sociedad de la Información. Política, Tecnología e Industria de los Contenidos,* CERA, Madrid, 1999;

-"Política del Tandem Clinton-Gore en Materia de Información: el Liderazgo de los EEUU", en CARIDAD SEBASTIÁN, Mercedes (Coordinadora), *La Sociedad de la Información. Política, Tecnología e Industria de los contenidos,* CERA Madrid, 1999.

MENÉNDEZ SEBASTIÁN, Eva María, "Principios de la responsabilidad *extra contractual* de la Administración Pública", QUINTANA LÓPEZ, Tomás (Dir.) y CASARES MARCOS, Anabelén (Coord.), *La Responsabilidad Patrimonial de la Administración Pública. Estudio general y ámbitos sectoriales*, Tirant lo Blanch, Valencia, 2009.

MESEGUER YEBRA, Joaquín, *El principio "non bis in idem" en el procedimiento administrativo sancionador*, BOSCH, Barcelona, 2000;

-*El Derecho de Acceso a los Documentos Administrativos y su Tutela*¸ BOSCH, Barcelona, 2000.

MESSÍA DE LA CERDA BALLESTEROS, Jesús Alberto, *La Cesión o Comunicación de Datos de Carácter Personal,* Thomson-Civitas, Madrid, 2003;

-"El derecho a la protección de datos y la dimensión colectiva de la libertad religiosa: a propósito de las sentencias de la Audiencia Nacional 396/2006 y 199/2006", *REPD,* nº 3, 2007;

-"Personalidad y protección de datos: el supuesto de las personas fallecidas", *Revista Crítica de Derecho Inmobiliario* nº 710, 2008;

-"Consideraciones sobre la regulación de los actos de cesión o comunicación de datos personales", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

MESTRE DELGADO, Juan Francisco, *El Derecho de Acceso a Archivos y Registros Administrativos. (Análisis del artículo 105.b) de la Constitución)*, Civitas, Madrid, 1998.

MESTRE DELGADO, Esteban, "El caso <<Eluana Englaro>> y el debate jurídico sobre el suicidio asistido", *La Ley Penal,* nº 60, 2009, http://revista-laleypenal.laley.es/

MIERES MIERES, Luis Javier, *Intimidad Personal y Familiar. Prontuario de Jurisprudencia Constitucional,* Aranzadi, Cizur Menor, 2002.

MIRA, J. J., PÉREZ-JOVER, V. y LORENZO, S., "Navegando en Internet en busca de información sanitaria: no es oro todo lo que reluce…", *Atención Primaria,* vol. 33, nº 7, 2004, http://www.doyma.es/

MIR PUIGPELAT, Oriol, *La Responsabilidad Patrimonial de la Administración Sanitaria. Organización, imputación y causalidad*, Civitas, Madrid, 2000.

MOLES PLAZA, Ramón J., *Derecho y Control en Internet. La Regulabilidad de Internet,* Ariel, Barcelona, 2004.

MONFORT PASTOR, Manuel, *El Derecho de Acceso de los Ciudadanos a la Documentación Municipal*, BAYER HNOS., Barcelona, 2004.

MONTAÑÉS PARDO, Miguel Angel, *La Presunción de Inocencia. Análisis doctrinal y jurisprudencial*, Aranzadi, Pamplona, 1999.

MORALES PRATS, Fermín, "Derecho a la Intimidad versus Tratamiento de Datos Sanitarios", Ponencia presentada en el marco del IX Congreso Derecho y Salud celebrado en Sevilla en noviembre del 2000, *DS*, vol. 9, nº 2, 2001;

-"Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", QUINTERO OLIVARES, Gonzalo (Dir.), *Comentarios a la Parte Especial del Derecho Penal,* Aranzadi-Thomson Reuters, Cizur Menor, 2009 (Octava edición).

MORANT VIDAL, Jesús, *Protección Penal de la Intimidad frente a las Nuevas Tecnologías (Estudio de los artículos 197 a 201 del Código Penal),* Práctica de Derecho, Valencia, 2003.

MORENA CATENA, Victor, "Ley de Conservación de Datos y Garantías Procesales", VVAA, *La Protección de Datos en la Cooperación Policial y Judicial,* Thomson-Aranzadi, Cizur Menor, 2008.

MORENA PÉREZ, Blanca, "Secreto Médico y práctica Psiquiátrica", CALCEDO ORDÓÑEZ, Alfredo (ed.), *Secreto Médico y Protección de Datos Sanitarios en la práctica Psiquiátrica,* Editorial Médica Panamericana, Madrid, 2000.

MORENO MOLINA, José Antonio y MAGÁN PERALES, José María, *La Responsabilidad Patrimonial de las Administraciones Públicas y, en especial, de las Corporaciones Locales,* El Consultor de los Ayuntamientos y de los Juzgados, Madrid, 2005.

MORENO VERNIS, Miguel, "Documentación Clínica: Organización, Custodia y Acceso", FERNÁNDEZ HIERRO, José Manuel (Coord.), *La Historia Clínica*, Comares, Granada, 2002.

MORO AGUADO, Jesús y TEJEDOR MUÑOZ, Jesús, *La Historia Clínica. Contenidos y Requerimientos en las Comunidades Autónomas*, Universidad de Valladolid, Salamanca, 2003.

MUNAR BERNAT, Pedro A., "El Tratamiento Automatizado de Datos Relativos a la Salud. Sus Límites en Derecho Comunitario y en Derecho Español", *RPJ*, CGPJ, nº 45, 1997.

MUÑOZ ARNAU, Juan Andrés, *Los Límites de los Derechos Fundamentales en el Derecho Constitucional Español*, Aranzadi, Pamplona, 1998.

MUÑOZ CONDE, Francisco, *Derecho Penal. Parte Especial*, Tiran lo Blanch, Valencia, 2004 (15ª edición).

MUÑOZ LLORENTE, José, *Libertad de Información y Derecho al Honor en el Código Penal de 1995*, Tirant lo Blanch, Valencia, 1999.

MUÑOZ MACHADO, Santiago, *La regulación de la red. Poder y Derecho en Internet*, Taurus, Madrid, 2000.

MURILLO de la CUEVA, Pablo Lucas, "La Protección de los Datos Personales ante el Uso de la Informática", *RFDUC*, nº15, 1989;

-*El Derecho a la Autodeterminación Informativa. La Protección de los Datos Personales Frente al Uso de la Informática,* Tecnos, Madrid, 1990;

-*Informática y Protección de Datos Personales (Estudio sobre la Ley Orgánica 5/1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal),* CEC., Madrid, 1993;

-"Avances Tecnológicos y Derechos Fundamentales. Los Riesgos del Progreso", VVAA, *Derechos Humanos y Nuevas Tecnologías,* XXI Cursos de Verano en Donosti-XIV Cursos Europeos, UPV-EHU, Colección Jornadas sobre Derechos Humanos nº 6, Ararteko, 2003;

-"El derecho fundamental a la protección de los datos relativos a la salud", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de protección de datos de carácter personal en el ámbito de la salud,* APDCat, Madrid, 2006;

-"La construcción del derecho a la autodeterminación informativa y las garantías para su efectividad", MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis, *El Derecho a la Autodeterminación Informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009;

-"Objeto de la Ley Orgánica de protección de datos de carácter personal", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

NARANJO DE LA CRUZ, Rafael, *Los Límites de los Derechos Fundamentales en las Relaciones entre Particulares: la Buena Fe,* CEPC, Madrid, 2000.

NAVALPOTRO NAVALPOTRO, Yolanda, "Ámbito de Aplicación de la Ley Orgánica de Protección de Datos de Carácter Personal", ALMUZARA ALMAIDA, Cristina (Coord.), *Estudio práctico de la protección de datos de carácter personal,* Lex Nova, Valladolid, 2007;

-"El deber de secreto", ALMUZARA ALMAIDA, Cristina (Coord.), *Estudio práctico sobre la protección de datos de carácter personal,* Lex Nova, Valladolid, 2007.

NAVALPOTRO, Yolanda, RODRÍGUEZ, María Luisa y TANÚS, Gustavo Daniel, "Críticas a la Nueva Ley Española de Protección de Datos Personales", http://www.geocities.com/SiliconValley/Circuit/4888/doctrina2.htm

NAVARRO LÓPEZ, Vicente, "Concepto Actual de la Salud Pública", VVAA, *La Salud Pública*, McGraw Hill, Madrid, 1998.

NEGROPONTE, Nicholas, *El Mundo Digital,* Ediciones B, Barcelona, 1995.

NICOLAS JIMÉNEZ, Pilar, "El concepto de dato médico y genético", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud*, APDCat, Madrid, 2006;

-La Protección Jurídica de los Datos Genéticos de Carácter Personal, Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia, de Derecho y Genoma Humano y Editorial COMARES, Bilbao-Granada, 2006

NICOLÁS ORTIZ, Carlos, *El Derecho a la Salud y los Derechos de los Enfermos*, Encuentro, Madrid, 1983.

NIETO, Alejandro, "Reforma Administrativa y Modernización de la Administración Pública: ¿Un Problema Pendiente?", *RVAP*, nº 23, 1989.

O´CALLAGHAN, Xavier, "El Concebido", *Compendio de Derecho Civil (*Tomo I), Edersa, 2004, en http://www.vlex.com/

OCHOA MONZO, Josep, "¿Hacia la Ciberadministración y el Ciberprocedimiento?", SOSA WAGNER, Francisco (Coord.), *El Derecho Administrativo en el Umbral del Siglo XXI (TomoI),* Tirant to Blanch, Valencia, 2000.

OLIVER, Francisco Eugenio y OLIVER, Luis Eugenio, "Protección de Datos. Análisis Comparado de la Legislación de algunos Países Europeos: Alemania, España, Francia y Gran Bretaña*", Boletín de la Facultad de Derecho*, nº7, UNED, 1994.

OROZCO PARDO, Guillermo, "Los Derechos de las Personas en la LORTAD", *IyD,* nº 6-7, UNED, 1994;

-"Notas acerca del Régimen Jurídico de los Ficheros de Datos Personales de Titularidad Universitaria", *IyD,* nº 23-26, UNED, 1998;

-"Notas Acerca de la Relación entre Informática y Propiedad Intelectual*", IyD*, nº 23-26, 1998;

-"La Protección de Datos en el Derecho Español a la Luz de la Reciente Jurisprudencia Constitucional", *AC,* nº 6, 4 al 10 de febrero 2002.

ORTEGA GIMÉNEZ, Alfonso, "Breve aproximación al futuro Reglamento de desarrollo de la Ley", *Datospersonales.org. Revista de la APDCM,* nº 30, 30 de noviembre 2007, en http://www.datospersonales.org/.

ORTEGA GUTIÉRREZ, David, *Derecho a la Información versus Derecho al Honor*, CEPC, Madrid, 1999;

-*Manual de Derecho de la Información,* CERA, Madrid, 2003.

ORTEGA Y GASSET, *La Rebelión de las Masas,* Revista de Occidente en Alianza Editorial, Madrid, 1981 (edición 8ª).

ORTEGO PÉREZ, Francisco, "Problemas derivados de las intervenciones corporales en la investigación criminal", *Diario La Ley,* nº 6049, 2004.

ORTÍ VALLEJO, Antonio, *Derecho a la Intimidad e Informática,* Comares, Granada, 1994;

-Derecho a la Intimidad e Informática. (Tutela de la Persona por el Uso de Ficheros y Tratamientos Informáticos de Datos Personales. Particular Atención a los Ficheros de Titularidad Privada), Comares, Granada, 1994

ORTIZ LIÑÁN, José, *Derechos y garantías del contribuyente ante la utilización por la Hacienda Pública de sus datos personales,* Comares, Granada, 2003.

OTALORA ARIÑO, Begoña, "Estrategias de Sistemas y Tecnologías de la Información del Sistema Sanitario Vasco", Ponencia presentada en el Seminario "Innovaciones en Tecnología de la Información en Salud", Segovia, 19 septiembre 2002.

OTERO GONZÁLEZ, Mª del Pilar, *Justicia y Secreto Profesional,* CERA, Madrid, 2001.

PAÉZ MAÑA, Jorge, *La protección de los Datos de Salud,* en http://www.iee.es/.

PALAO TABOADA, Carlos, *El Derecho a no Autoinculparse en el Ámbito Tributario*, Thomson-Civitas, Cizur Menor, 2008.

PALOMAR OLMEDA, Alberto, "Los Derechos Personales en el Ámbito de la Protección de Datos", *REPD,* nº 2, 2007.

PALOMAR OLMEDA, Alberto y PÉREZ GONZÁLEZ, Carmen, "La Protección de Datos: su marco constitucional e internacional y el contexto del nuevo Reglamento", PALOMAR OLMEDA, Alberto (Coord.), *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de*

diciembre, de Protección de Datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre), Thomson-Civitas, Cizur Menor, 2008.

PANTALEÓN, Fernando, *Responsabilidad médica y responsabilidad de la Administración*, Civitas, Madrid, 1995.

PARDO FALCON, Javier, "Los derechos fundamentales como límites de los poderes jurídicos del empresario. (Un comentario de las SSTC 99/1994, 11 de abril, y 6/1995, de 10 de enero), *REDC*, nº 49, 1997.

PAREJO ALFONSO, Luciano, "El contenido esencial de los derechos fundamentales en la jurisprudencia constitucional: a propósito de la Sentencia del Tribunal Constitucional de 8 de abril de 1981", *REDC,* nº 3, 1981.

PELLEJERO GARCÍA, Carlos, "Informes de Alta y otra documentación clínica en la Ley 41/2002 de 14 de noviembre", GONZÁLEZ SALINAS, Pedro y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Thomson-Civitas, Madrid, 2004.

PEMAN GAVIN, Juan, *Derecho a la Salud y Administración Sanitaria*, Real Colegio de España, Bolonia, 1989.

PERA VERDAGUER, Francisco, *Comentarios a la Ley de lo Contencioso Administrativo. Ley 29/1998, de 14 de julio. Con Jurisprudencia y Formularios,* BOSCH, Barcelona, 2004.

PÉREZ-CAMPANERO ATANASIO, Juan Antonio, "La Gestión de la Seguridad en los Sistemas de Información y de las Comunicaciones"*,* VVAA, *Informe SEIS. La Seguridad y Confidencialidad de la información clínica,* 12/12/2000, http://www.seis.es/.

PÉREZ GÁLVEZ, Juan Francisco, "Administración Sanitaria y Telemedicina"*, AA*, XXXI, 2003, http://www.laley.net/

PÉREZ GÓMEZ, José María, "Protección de datos personales de salud en materia de información sanitaria", VVAA, *Protección de datos e investigación médica,* Aranzadi y Thomson-Reuters, Cizur Menor, 2009.

PÉREZ LUÑO, Antonio Enrique, "La Protección de la Intimidad frente a la Informática en la Constitución Española de 1978", *REP,* nº 9, 1979;

-"Informática y Libertad. Comentario al artículo 18.4 de la Constitución Española*", REP (Nueva Época*), nº24, noviembre-diciembre, 1981;

-*Los Derechos Fundamentales*, Tecnos, Madrid, 1984;

-"La Defensa del Ciudadano y la Protección de Datos", *RVAP*, nº 14, 1986;

-*Nuevas Tecnologías, Sociedad y Derecho,* Los Libros de Fundesco, Madrid, 1987;

-“Intimidad y Protección de Datos Personales: del “Habeas Corpus” al “Habeas Data””, en *Estudio sobre el Derecho a la intimidad,* Tecnos, 1992;

-*Manual de Informática y Derecho,* Ariel, Barcelona, 1996;

-*Derechos Humanos, Estado de Derecho y Constitución,* Tecnos, Madrid, 1996;

-*¿Ciberciudadaní@ o ciudadanía.com?,* Gedisa, Barcelona, 2004;

-*Dimensiones de la Igualdad*, Dykinson, Madrid, 2005;

-”Derecho y nuevas tecnologías: impacto de la red en las libertades”, *RFDUG,* nº 8, 2005;

-La Tercera Generación de Derechos Humanos, Thomson-Aranzadi, Cizur Menor, 2006;

-“El Consentimiento de los menores”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

PÉREZ-MADRID, Francisca, “La autonomía de las confesiones y entidades religiosas en materia de protección de datos”, TRONCOSO REIGADA, Antonio (Dir.) *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

PÉREZ ROYO, Javier, *Curso de Derecho Constitucional*, Marcial Pons, Madrid, 1997.

PÉREZ VELASCO, Mª del Mar, “La Potestad Inspectora y los Ficheros Públicos”, ponencia presentada en el I Encuentro de las Agencias Autonómicas de Protección de Datos, celebrado en Getafe el 2 de noviembre de 2004;

-“Los Ficheros Públicos”, en la revista electrónica de la APDCM *datospersonales.org* nº 16, 22 de julio de 2005, en http://www.datospersonales.org/;

-“Los ficheros públicos”, APDCM, *Estudios sobre Administraciones Públicas y Protección de Datos Personales (I Encuentro entre Agencias Autonómicas de Protección de Datos Personales)*, Thomson-Civitas y APDCM, Madrid, 2006.

PICAZO SENTÍ, Pedro y CHAVELI DONET, Eduard, “El tratamiento por el empresario de los datos de salud relativos a los trabajadores”, *REDI* nº 46, 2002, http://vlex.com

PIÑAR MAÑAS, José Luís, “El peor riesgo para nuestros datos personales es ignorar cómo se usan”, *El País,* 30 de diciembre de 2003.

-“El Porqué de un Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos”, *REPD,* nº 3, 2007;

-"Novedades en relación con la figura del encargado del tratamiento", ZABÍA DE LA MATA, Juan (Coord.), *Protección de Datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008;

-"Nuevas tecnologías, Administración Pública y protección de datos personales", VVAA, *Derechos Fundamentales y otros estudios. Homenaje al prof. Dr. Lorenzo Martín-Retortillo (Volumen I)*, Gobierno de Aragón, Cortes de Aragón, El Justicia de Aragón, Caja Inmaculada, Ibercaja y Facultad de Derecho de la Universidad de Zaragoza, Zaragoza, 2008;

-"Protección de Datos: origen, situación actual y retos de futuro", MURILLO DE LA CUEVA, Pablo Lucas y PIÑAR MAÑAS, José Luis, *El Derecho a la Autodeterminación Informativa,* Fundación Coloquio Jurídico Europeo, Madrid, 2009;

-"Concepto de dato de carácter personal", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010;

-"Transparencia y protección de datos: las claves de un equilibrio necesario", GARCÍA MACHO, Ricado (ed.), *Derecho administrativo de la información y administración transparente*, Marcial Pons, Madrid-Barcelona-Buenos Aires, 2010.

PISARELLO, Gerardo, *Los Derechos Sociales y sus Garantías. Elementos para una reconstrucción,* Trotta, Madrid, 2007;

-"El Derecho a la Vivienda como derecho social: implicaciones constitucionales", *RCDP*, nº 38, 2009.

POMED SÁNCHEZ, Luis, "El acceso a los archivos administrativos: el marco jurídico y la práctica administrativa", *RAP,* nº 142, 1997.

PONS RAFOLS, Xavier, "La salud como objeto de cooperación y regulación jurídica internacional", PONS RAFOLS, Xavier (ed.), *Salud Pública mundial y Derecho internacional*, Marcial Pons, Madrid, 2010.

POULLET, Yves, "Flujos de Datos Transfronterizos y Extraterritorialidad: la postura europea", *REPD,* nº 1, 2006.

PRADA FERNÁNDEZ DE SANMAMED, José Luis, "Revisión de los principios rectores de la política social y económica y de su actual realidad jurídico-constitucional", *REP*, nº 122, 2003.

PRIETO SANCHIS, Luis, *Estudios sobre Derechos Fundamentales*, Debate, Madrid, 1990.

PUENTE ESCOBAR, Agustín, "Ámbito objetivo de aplicación; ámbito territorial de aplicación; tratamientos excluidos", ZABÍA DE LA MATA, Juan (Coord.), *Protección de Datos. Comentarios al Reglamento*, Lex Nova, Valladolid, 2008;

-“Derechos de las personas”, PALOMAR OLMEDA, Alberto (Coord.), *Comentario al Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal (aprobado por RD 1720/2007, de 21 de diciembre)*, Thomson Civitas, Cizur Menor, 2008;

-“Consentimiento del afectado y deber de información”, MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Protección de Datos. Comentarios al Reglamento de desarrollo de la LOPD*, Tirant lo Blanch, Valencia, 2009.

PULIDO QUECEDO, Manuel, *Responsabilidad Patrimonial del Estado*, Aranzadi-Thomson Reuters, Cizur Menor, 2010 (2ª edición).

PUYOL MONTERO, Javier, “Los derechos de acceso, rectificación, cancelación y oposición”, ZABÍA DE LA MATA, Juan (Coord.), *Protección de Datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008;

-“Derecho a Indemnización”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

QUERALT JIMÉNEZ, Joan J., *Derecho Penal español. Parte especial,* Atelier, Barcelona, 2008.

QUINTANA LÓPEZ, Tomás (Dir.) y CASARES MARCOS, Anabelén (Coord.), *La Responsabilidad Patrimonial de la Administración Pública. Estudio general y ámbitos sectoriales*, Tirant lo Blanch, Valencia, 2009.

RALLO LOMBARTE, Artemi y MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Derecho y Redes Sociales,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

RAMÍREZ NEILA, Nieves, “Accesos legítimos a las historias clínicas electrónicas”, VVAA, *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica,* Aranzadi y Thomson Reuters, Cizur Menor, 2009.

RAMÍREZ REYNA, Nieves, “Accesos legítimos a las historias clínicas electrónicas”, VVAA, *El Derecho a la Protección de Datos en la Historia Clínica y la Receta Electrónica,* Aranzadi y Thomson-Reuters, Cizur Menor, 2009

RAMS RAMOS, Leonor, *El Derecho de Acceso a Archivos y Registros Administrativos,* Reus, Madrid, 2008.

REBOLLO DELGADO, Lucrecio, *El Derecho Fundamental a la Intimidad,* Dykinson, Madrid, 2005 (segunda edición);

-*Derechos Fundamentales y Protección de Datos,* Dykinson, Madrid, 2004.

REBOLLO PUIG, Manuel, “Juridicidad, Legalidad y Reserva de Ley como Límites a la Potestad Reglamentaria del Gobierno”, *RAP* nº 125, 1991.

REDONDO ANDREU, Ignacio, "El principio de *Non Bis In Idem*", VVAA, *Manual de Derecho Administrativo Sancionador* (Tomo I), Ministerio de Justicia y Thomson Reuters-Aranzadi, Cizur Menor, 2009.

REESE J., KUBICEK H., LANGE B-P, LUTTERBECK B. y REESE V., *El Impacto Social de las Modernas Tecnologías de la Información,* Fundesco/Tecnos, Madrid, 1982.

REGLERO CAMPOS, L. Fernando, "Artículo 10", REGLERO CAMPOS, L. Fernando (Coord.), *Ley de Contrato de Seguro*, Thomson-Aranzadi, Cizru Menor, 2007.

REIGOSA, Luis; CASTILLA, Virgilio y BLANCO, Angel, "Desde la Informática Clínica hasta el Soporte del Proceso Asistencial"*,* Revista Calidad Asistencial, vol. 17, nº 3, 2002, http://www.doyma.es/.

REIG REDONDO, Juan, "El Futuro de la Sanidad Pasará por la Figura del Médico on-line"*, IyS,* nº 26, mayo-junio 2000, http://www.seis.es/.

REQUEJO NAVEROS, Mª Teresa, *El Delito de Revelación de Secreto Médico y la Protección Penal de la Información Genética,* Colex, Madrid, 2006

-"El Derecho a no saber: fundamento y necesidad de protección penal", *Diario La Ley* nº 6401, 2006, http://diariolaley.laley.es

REQUERO IBÁÑEZ, José Luis, "El Consentimiento Informado y la Responsabilidad Patrimonial de las Administraciones", *AA,* nº 31, 29 de julio al 4 de agosto de 2002.

RIGO VALLBONA, José, *El Secreto Profesional de Abogados y Procuradores,* BOSCH, Barcelona, 1988.

RÍOS INSUA, David, FERNÁNDEZ, Eugenio y RÍOS, Jesús María, "Más Allá del Gobierno Electrónico: hacia la Democracia Electrónica"*, RAPDCM*, nº 8, 30 marzo 2004, http://www.datospersonales.org/.

RIPOL CARULLA, Santiago, "La Protección de los Datos Médicos y Genéticos en la Normativa del Consejo de Europa (Partes I y II*)", RDGH*, Fundación BBV-Diputación Foral de Bizkaia, nº 5, julio-diciembre, 1996;

-"El Tratamiento de los Datos Médicos y Genéticos en la Administración Sanitaria"*,* HEREDERO HIGUERAS, Manuel (Coord.), *El Derecho de la intimidad y a la privacidad y las Administraciones Públicas,* Colección Xornadas e Seminiarios, nº 24, Xunta de Galicia, 1999;

-"Incidencia en la Jurisprudencia del TC de las sentencias del TEDH que declaran la vulneración por España del CEDH*", REDC,* nº 79, 2007;

-El Sistema Europeo de Protección de los Derechos Humanos y el Derecho Español, Atelier, Barcelona, 2007.

RIVERO LAMAS, Juan, *Protección de la Salud y Estado Social de Derecho*, Real Academia de Medicina, Zaragoza, 2000;

RODRÍGUEZ-ARMAS, Magdalena Lorenzo, *Análisis del Contenido Esencial de los Derechos Fundamentales enunciados en el art. 53.1 de la Constitución española*, Comares, Granada, 1996.

RODRÍGUEZ DE SANTIAGO, José María, "Artículo 53.3. La forma de vincular de los preceptos del Capítulo Tercero del Título Primero de la Constitución Española", CASAS BAAMONDE, María Emilia, RODRÍGUEZ PIÑERO Y BRAVO FERRER, Miguel (Coords.), *Comentarios a la Constitución Española*, Wolters Kluwer, Madrid, 2008;

-"Las garantías constitucionales de la propiedad y de la expropiación forzosa a los treinta años de la Constitución Española", *RAP,* nº 177, 2008.

RODRÍGUEZ ESCANCIANO, Susana, *El Derecho a la Protección de Datos Personales de los Trabajadores: nuevas perspectivas,* Bomarzo, Albacete, 2009.

RODRÍGUEZ LÓPEZ, Pedro, *La Autonomía del Paciente: información, consentimiento y documentación clínica*, Dilex, Paracuellos del Jarama, 2004;

-Nuevas Formas de Gestión Hospitalaria y Responsabilidad Patrimonial de la Administración, Dykinson, Madrid, 2004.

RODRÍGUEZ-PIÑERO, Miguel y DEL REY, Salvador, "Informe Español", MARZAL, Antonio (ed.), *Protección de la salud y Derecho Social,* J.M. BOSCH editor y ESADE FACULTAD DE DERECHO, Barcelona, 1999.

ROIG, Francesc y SAIGÍ, Francesc, "Dificultades para incorporar la telemedicina en las organizaciones sanitarias: perspectivas analíticas", *Gaceta Sanitaria* vol. 23 nº 2, 2009, en http://www.doyma.es/.

ROMEO CASABONA, Carlos María, *Información y documentación clínica: su tratamiento jurisprudencial,* Ministerio de Sanidad y Consumo, Madrid, 2000;

-"La protección de datos de salud en la investigación biomédica", VVAA, *Protección de datos e investigación médica*, Aranzadi y Thomson-Reuters, Cizur Menor, 2009.

-"Persona identificada o identificable, el afectado o interesado y el procedimiento de disociación en la protección de datos de carácter personal", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*", Civitas y Thomson-Reuters, Cizur Menor, 2010.

ROMERO COLOMA, Aurelia María, *Libertad de Información frente a otros derechos en conflicto: Honor, intimidad y presunción de inocencia*, Civitas, Madrid, 2000;

-"Pruebas biológicas de paternidad, colisión con derechos fundamentales y consentimiento de los progenitores", *Diario La Ley,* nº 7158, 2009.

-*Identidad genética frente a intimidad y pruebas de paternidad*, BOSCH, Barcelona, 2009.

ROVIRA VIÑÁS, Antonio, "Introducción", ROVIRA VIÑÁS, Antonio (Dir.), *Comentarios a la Ley Orgánica del Defensor del Pueblo*, Aranzadi, Cizur Menor, 2002.

RUBÍ NAVARRETE, Jesús, Los Códigos Tipo: la Alternativa de la Autorregulación", *AIA*, nº 35, abril 2000;

-"La Autorregulación, Alternativa a la Falta de Definición Legal de los Datos de Salud*", Actualidad de Derecho Sanitario*, nº 94, mayo 2003;

-"La Protección Especial de los Datos Sanitarios: Requisitos de la Ley y Régimen Sancionador", Ponencia presentada en el IV Congreso de Responsabilidad Sanitaria celebrado en Madrid el 26 y 27 de febrero de 2003, http://www.actualderechosanitario.com/;

-"Experiencias y criterios de la AEPD sobre los datos personales de la salud", RIPOL CARULLA, Santiago (ed.) y BACARIA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud*", APDCat y Marcial Pons, Madrid, 2006.

-"Códigos Tipo", MARTÍNEZ MARTÍNEZ, Ricard (Coord.), *Protección de Datos. Comentarios al Reglamento de Desarrollo de la LOPD,* Tirant lo Blanch, Valencia, 2009.

RUEDA MARTÍN, Mª Ángeles, *Protección Penal de la Intimidad Personal e Informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal),* Atelier, Barcelona, 2004.

RUIZ CARRILLO, Antonio, *La Protección de los Datos de Carácter Personal*, BOSCH, Barcelona, 2001;

-*Manual Práctico de Protección de Datos,* BOSCH, Barcelona, 2005;

-*El Tratamiento de los Datos Personales en los Documentos de Seguridad,* BOSCH, Barcelona, 2008.

RUIZ MARTÍNEZ, Esteban, "España: el Derecho a Controlar la Información Personal", *REDI*, nº 49, agosto 2002, en http://www.premium.vlex.com/.

SAIZ ARNAIZ, Alejandro, *La Apertura Constitucional al Derecho Internacional y Europeo de los Derechos Humanos. El artículo 10.2 de la Constitución Española*, CGPJ, Madrid, 1999.

SAÍZ PEÑA. Carlos Alberto, "La externalización de los Servicios TIC de una Organización. El caso práctico del *outsourcing* del Servicio de Atención a Usuarios. Aproximación a los aspectos de protección de datos, riesgos contractuales y análisis de riesgos de seguridad de la información", *REPD,* nº 5, 2008.

SALINAS ALCEGA, Sergio, El Consejo de Europa. Su protagonismo en la construcción de la <<Gran Europa>> y sus aportaciones al progreso del Derecho Internacional Público, Ministerio de Asuntos Españoles, Madrid, 1999.

SALVADOR CODERCH, Pablo y CASTIÑEIRA PALOU, María Teresa, *Prevenir y Castigar. Libertad de Información y expresión, tutela del honor y funciones del derecho de daños*, Marcial Pons, Madrid, 1997.

SAMPRÓN LÓPEZ, David, *Los Derechos del Paciente a través de la Información y la Historia Clínica,* Edisofer, Madrid, 2002.

SÁNCHEZ BRAVO, Álvaro A., "La Regulación de los Datos Sensibles en la LORTAD*", Informática y Derecho*, nº 6-7, UNED, 1994;

-"Una Política Comunitaria de Seguridad en Internet"*, Diario La Ley* nº 5414, 8 noviembre 2001, http://www.laley.net/;

-"El Control de la Red"*, Diaro la Ley*, nº 5686, 30 diciembre 2002, http://www.laley.net/;

-"El Convenio del Consejo de Europa sobre Cibercrimen: Control vs. Libertades Públicas"*, Diario La Ley*, nº 5528, 22 abril 2002, http://www.laley.net/.

SÁNCHEZ CALERO, Fernando, "Artículo 10", SÁNCHEZ CALERO, Fernando (Dir.), *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, 8 de octubre, y a sus modificaciones*, Aranzadi, Cizur Menor, 2001.

-"Artículo 11", SÁNCHEZ CALERO, Fernando (Dir.), *Ley de Contrato de Seguro. Comentarios a la Ley 50/1980, 8 de octubre, y a sus modificaciones*, Aranzadi, Cizur Menor, 2001.

SÁNCHEZ CARAZO, Carmen, *La Intimidad y el Secreto Médico,* Díaz de Santos, Madrid, 2000;

-*Noticias Lopdate*, del 20/05/2003, en http://www.lopdate.com/.

SÁNCHEZ CARAZO, Juan María y SÁNCHEZ CARAZO, Carmen, *Protección de Datos de Carácter Personal Relativos a la Salud,* APD, Madrid 1999.

SÁNCHEZ CARO, Javier y ABELLÁN, Fernando, *Telemedicina y Protección de Datos Sanitarios,* Comares, Granada, 2002;

-Derechos y Deberes de los Pacientes. Ley 41/2002 de 14 de noviembre: Consentimiento Informado, Historia Clínica, Intimidad e Instrucciones Previas, Comares, Granada, 2003;

-Datos de Salud y Datos Genéticos. Su Protección en la Unión Europea y en España, Comares, Granada, 2004.

SÁNCHEZ CARO, Javier, "El uso y acceso a la historia clínica electrónica (HCE) y la protección de datos", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

SÁNCHEZ CARO, Jesús y SÁNCHEZ-CARO, Javier, *El Médico y la Intimidad,* Díaz de Santos, Madrid, 2001.

SÁNCHEZ FERRIZ, Remedio, *El Derecho a la Información*, Cosmos, Valencia, 1974;

-"El Derecho de la Información como ordenación", VVAA, *Derecho de la Información,* Ariel, Barcelona, 2003;

-*Delimitación de las libertades informativas,* Tirant lo Blanch, Valencia, 2004.

SÁNCHEZ FIERRO, Julio, "Los Nuevos Avances en la Medicina y sus Repercusiones en la Relación Médico-Paciente"*,* http://www.aeds.org/.

SÁNCHEZ GONZÁLEZ, Santiago, "Los límites de los derechos", SÁNCHEZ GONZÁLEZ, Santiago (Dir.), *Dogmática y práctica de los Derechos Fundamentales*, Tirant lo Blanch, Valencia, 2006.

SÁNCHEZ GOYANES, Enrique, *Constitución Española Comentada,* Thomson-Paraninfo, Madrid, 2005.

SÁNCHEZ MECA, Diego, "Cuestiones Eficaces en torno a la Libertad Informática"*, IyD,* nº 19-22, UNED, 1998.

SÁNCHEZ MORÓN, Miguel, "Función Administrativa y Constitución", PREDIERI, Alberto y GARCÍA de ENTERRÍA, Eduardo (Dirs.), *La Constitución Española de 1978*, Civitas, Madrid, 1984;

-*Derecho Administrativo. Parte General,* Tecnos, Madrid, 2006 (segunda edición);

-*Derecho Administrativo. Parte General*, Tecnos, Madrid, 2009 (quinta edición).

SÁNCHEZ SAUDINÓS, José Manuel, *Los Colegios Profesionales en el Ordenamiento Constitucional,* Centro de Estudios Constitucionales, Madrid, 1996.

SANCHO VILLA, Diana, "Normas corporativas vinculantes (*binding corporate rules)*: aspectos sustantivos y de cooperación internacional de autoridades", *REPD,* nº 4, 2008;

-*Negocios Internacionales de Tratamiento de Datos Personales*, Civitas-Thomson Reuters, Cizur Menor, 2010.

SAN JULIÁN PUIG, Verónica, *El Objeto del Contrato,* Aranzadi, Pamplona, 1996;

-“Los Principios Generales de la Ley 41/2002”, LEÓN SANZ, Pilar (ed.), *La Implantación de los Derechos del Paciente*, EUNSA, Pamplona, 2004.

SANJURJO REBOLLO, Beatriz, *Manual de derecho de la información (una perspectiva legal para un mundo cada día más mediático),* Dykinson, Madrid, 2009.

SANTAMARÍA PASTOR, Juan Alfonso, *Principios de Derecho Administrativo (Vol I)*, CERA, Madrid, 2002.

SANTOS GARCÍA, Daniel, *Nociones Generales de la Ley Orgánica de Protección de Datos*, Tecnos, Madrid, 2005.

SANTOS VIJANDE, Jesús María, *La Protección Jurisdiccional, Civil y Penal, del Honor, la Intimidad y la Propia Imagen,* Thomson-Civitas, Cizur Menor, 2005.

SANZ CALVO, Lurdes, “Calidad de los datos”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia,* Lex Nova, Valladolid, 2008;

-“Consentimiento del afectado”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y comentario de su jurisprudencia,* Lex Nova, Valladolid, 2008;

-“Datos relativos a la salud”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008;

-“Deber de secreto”, LESMES SERRANO, Carlos (Coord.), *La Ley de Protección de Datos. Análisis y Comentario de su Jurisprudencia*, Lex Nova, Valladolid, 2008.

SANZ DÍAZ-PALACIOS, J. Alberto, *Derecho a no autoinculparse y delitos contra la Hacienda Pública,* Colex, Madrid, 2004.

SANZ URETA, Jokin y HUALDE TAPIA, Sebastián, “Aspectos Técnicos de la Seguridad en la Información Sanitaria”*,* VVAA, *Informe SEIS. La seguridad y Confidencialidad de la Información Clínica,* 12/12/2000, http://www.seis.es/.

SARAZA JIMENA, Rafael, *Libertad de Expresión e Información Frente a Honor, Intimidad y Propia Imagen*, Aranzadi, Pamplona, 1995.

SARMIENTO RAMÍREZ-ESCUDERO, Daniel, *El Control de Proporcionalidad de la Actividad Administrativa*, Tirant lo Blanch, Valencia, 2004.

SENDEN, Linda, *Soft Law in European Community Law,* HART, Oxford, 2004.

SENDÍN GARCÍA, Miguel Ángel, “El documento”, SENDÍN GARCÍA, Miguel Ángel y GÓMEZ DÍAZ, Raquel (Dirs.), *Régimen jurídico de los documentos. Aspectos administrativos, civiles, penales y procesales,* Comares, Granada, 2009;

-"El expediente administrativo", SENDÍN GARCÍA, Miguel Ángel y GÓMEZ DÍAZ, Raquel (Dir.), *Régimen jurídico de los documentos. Aspectos administrativos, civiles, penales y procesales,* Comares, Granada, 2009.

SEOANE PRADO, Javier, "Información Clínica"*, EDJ*, nº 7 vol. 1, 1997.

SEOANE RODRÍGUEZ, José Antonio, "De la Intimidad Genética al Derecho a la Protección de Datos Genéticos, La Protección Iusfundamental de los Datos Genéticos en el Derecho Español (a propósito de las SSTC 290/00 y 292/00, de 30 de noviembre) (parte II*)", RDGH*, Fundación BBVA y Diputación Foral de Bizkaia, nº 17, julio-diciembre 2002;

-"¿A quién pertenece la Historia Clínica? Una propuesta armonizadora desde el lenguaje de los derechos", *DS*, vol 10 nº 2, 2002

-"El Significado de la Ley Básica de Autonomía del Paciente (Ley 41/2002, de 14 de noviembre) en el Sistema Jurídico-Sanitario Español. Una Propuesta de Interpretación", *DS.* vol. 12, nº 1, 2004.

SEOANE, José Antonio, HERNANDO ROBLES, Pablo, DE ASÍS CUBAS y GONZÁLEZ, José Francisco, "Historia clínica y derechos fundamentales: una reflexión sobre las anotaciones subjetivas", *Datospersonales.org* Nº 21, 2006.

SEOANE SPIEGELBERG, José Luis, *La Prueba en la Ley de Enjuiciamiento Civil 1/2000. Disposiciones Generales y Presunciones*, Aranzadi, Cizur Menor, 2002.

SERRANO DE PABLO VALDENEBRO, Luis, "Las Transferencias Internacionales de Datos", ZABÍA DE LA MATA, Juan (Coord.), *Protección de Datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008.

SERRANO PÉREZ, María Mercedes, *El Derecho Fundamental a la Protección de Datos: Derecho Español y Comparado,* Civitas, Madrid, 2003;

-"Los derechos de rectificación y cancelación", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas y Thomson-Reuters, Cizur Menor, 2010.

SIERRA NAVA, José María, *El Consejo de Europa,* Instituto de Estudios Políticos, Madrid, 1957.

SILBER, Denise, *The case for eHealth,* presented at the eHealth Conference, Cork-Ireland, 5-6 may 2003, http://europa.eu.int/.

SILVA SÁNCHEZ, Jesús María, "Los <<Documentos de Instrucciones Previas>> de los pacientes (artículo 11.1 Ley 41/2002) en el contexto del debate sobre la (in)disponibilidad de la vida", *Diario La Ley*, nº 5840, 2003.

SIMITIS, Spiros, *Revisiting Sensitive Data,* 1999, http://www.coe.int/.

SOLER-GONZÁLEZ, J.; RIBA TORRECILLAS, D., RODRÍGUEZ ROSICH, A; SANTAFÉ SOLER, P.y BUTI SOLE, M., "Aplicaciones de Tecnología Digital en la Medicina Rural"*, SEMERGEN*, vol. 30, nº 4, 2004, http://www.doyma.es/.

SOLERNOU VIÑOLAS, Ágata, "Aspectos legales y éticos del tratamiento de la información sanitaria en el contexto europeo", RIPOL CARULLA, Santiago (ed.) y BACARÍA MARTRUS, Jordi (Coord.), *Estudios de Protección de Datos de Carácter Personal en el Ámbito de la Salud,* Marcial Pons y APDCat, Madrid y Barcelona, 2006.

SOMMERMANN, Karl-Peter, "La exigencia de una Administración transparente en la perspectiva de los principios de Democracia y del Estado de Derecho", GARCÍA MACHO, Ricardo (ed.), *Derecho administrativo de la información y administración transparente*, Marcial Pons, Madrid-Barcelona-Buenos Aires, 2010.

SOUVIRÓN, José María, *Naturaleza y Caracteres de los Colegios Profesionales: Notas para una Ley Reguladora,* Instituto Nacional de Prospectiva, Madrid, 1980;

-"En torno a la Juridificación del Poder Informativo del Estado y el Control de Datos por la Administración"*, RVAP*, nº 40, 1994.

STERN, Klaus, *Jurisdicción constitucional y Legislador,* Dykinson, Madrid, 2009.

SUÑÉ LLINAS, Emilio y VILLAR PALASÍ, José Luis, "El Estado de Derecho y la Constitución", ALZAGA VILLAAMIL, Oscar (Dir.), *Comentarios a la Constitución Española de 1978 (Tomo I)*, Cortes Generales. Editoriales de Derecho Reunidas, Madrid, 1996.

TAJADURA TEJADA, Idoia, "La Protección de la Salud", TAJADURA TEJADA, Javier (Dir.), *Los Principios Rectores de la Política Social y Económica*, Biblioteca Nueva, Madrid, 2004.

TARODO SORIA, Salvador, "La doctrina del consentimiento informado en el ordenamiento jurídico norteamericano", *DS,* vol. 14 nº1, 2006.

TASCÓN LÓPEZ, Rodrigo, *El Tratamiento por la Empresa de Datos Personales de los Trabajadores. Análisis del Estado de la Cuestión,* Thomson-Civitas y APDCM, Cizur Menor, 2005.

TÉLLEZ AGUILERA, Abel, *Nuevas Tecnologías, Intimidad y Protección de Datos. Estudio Sistemático de la Ley Orgánica 15/1999,* Edisofer, Madrid, 2001;

-Telemedicina y Protección de Datos Sanitarios. Aspectos Legales y Éticos, Comares, Granada, 2002;

-La Protección de Datos en la Unión Europea. Divergencias Normativas y Anhelos Unificadores, Edisofer, Madrid, 2002.

TERRADILLOS ORMAETXEA, Edurne, *Principio de Proporcionalidad, Constitución y Derecho del Trabajo*, Tirant lo Blanch, Valencia, 2004.

TOFFLER, Alvin, *La tercera ola,* Plaza y Janes, Barcelona, 1980.

TOMÁS, Rafael M., "La implantación de la Historia Clínica Electrónica no es sólo un Problema Electrónico"*, Diario Médico*, 30 mayo 2003, http://www.diariomedico.com/.

TONIATTI, Roberto, "Liberad Informática y Derecho a la Protección de Datos Personales: Principios de Legislación Comparada", *RVAP*, nº29, 1991.

TORNE-DONBIDAU JIMÉNEZ, José y CASTILLO BLANCO, Federico, A., "Informática y Protección de la Privacidad del Individuo (I)", *AA*, nº 22, 31 mayo-6 junio, 1993-2.

TRONCOSO REIGADA, Antonio, *Guía de protección de datos personales para Servicios Sanitarios Públicos (Introducción y Presentación)*, Thomson-Civitas y APDCM, Madrid, 2004;

-*Administración electrónica y Protección de Datos en Regiones y Ciudades Europeas (Introducción),* APDCM, Madrid, 2006.

-*Protección de datos personales para Servicios Sanitarios Públicos (Introducción y Presentación)*, Thomson-Civitas y APDCM, Madrid, 2008.

-"Transparencia administrativa y protección de datos personales", VVAA, *Transparencia administrativa y Protección de Datos Personales. V Encuentro entre Agencias Autonómicas de Protección de Datos Personales,* Thomson-Civitas y APDCM, Madrid, 2008;

-"El principio de calidad de los datos", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010;

-"La comunicación de datos personales", TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010;

-*La Protección de Datos Personales. En Busca del Equilibrio*, Tirant lo Blanch, Valencia, 2010.

UGARTEMENDIA ECEIZABARRENA, Juan Ignacio, *El Derecho Comunitario y el Legislador de los Derechos Fundamentales. Un estudio de la influencia comunitaria sobre la fundamentalidad de los derechos constitucionales*, IVAP-HAEE, Oñati, 2001.

ULL PONT, Eugenio, *Derecho Público de la Informática (Protección de Datos de Carácter Personal),* UNED, Madrid, 2000.

URÍAS, Joaquín, *Lecciones de Derecho de la Información,* Tecnos, Madrid, 2003.

VALCÁRCEL TEIJEIRO, Néstor, "Protección de Datos de Salud e Investigación Hospitalaria", VVAA, *Protección de datos e investigación médica,* Aranzadi y Thomson-Reuters, Cizur Menor, 2009.

VALERO TORRIJOS, Julián, “Administración Pública, Ciudadanos y Nuevas Tecnologías”, SOSA WAGNER, Francisco (Coord.), *El Derecho Administrativo en el Umbral del siglo XXI (Tomo III),* Tirant to Blanch, 2000;

-El Régimen Jurídico de la e-administración. El Uso de los Medios Informáticos y Telemáticos en el Procedimiento Administrativo, Comares, Granada, 2004;

-“Acceso a los servicios y a la información por medios electrónicos”, GAMERO CASADO, Eduardo y VALERO TORRIJOS, Julián (Coords.), *La Ley de Administración Electrónica. Comentario Sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, Thomson-Aranzadi, Cizur Menor, 2008.

VALERO TORRIJOS, Julián y LÓPEZ PELLICER, Juan Antonio, “Algunas Consideraciones sobre el Derecho a la Protección de los Datos Personales en la Actividad Administrativa”, *RVAP*, nº 59, 2000.

VANDERBERGME, G.P.V., “Law and Infomation Technology: Object and Scope”, VVAA, *Advanced Topics of Law and Information Technology,* Kluwer, Deventer (Países Bajos), 1989.

VAQUERO PUERTA, José Luis, *Salud Pública*, Pirámide, Madrid, 1988.

VARELA SUANCES-CARPEGNA, “La naturaleza jurídica del Defensor del Pueblo”, *REDC,* nº 3, 1983.

VELA SÁNCHEZ-MERLO, Cayetana, “La Privacidad de los Datos en las Redes Sociales”, *REPD,* nº 5, 2008.

VELÁZQUEZ BAUTISTA, Rafael, *Protección Jurídica de Datos Personales Automatizados,* Colex, Madrid, 1993;

-100 interrog@ntes fundamentales en Derecho de Tecnologías de la Información y las Comunicaciones, Colex, Madrid, 2004.

VELEIRO, Belén, *Protección de Datos de Carácter Personal y Sociedad de la Información,* Boletín Oficial del Estado, Madrid, 2008.

VERDAGUER LÓPEZ, Jordi y BERGAS JANÉ, Mª Antonia, *Prontuario protección de datos*, CISS, Valencia, 2009.

VERDÚ, Vicente, *Las Autopistas de la Información y sus Pistas Sociológicas,* en Ponencias del Curso de Verano del Escorial, *Autopistas de la Información: el Reto del siglo XXI,* julio 1995, Universidad Complutense, 1995.

VERDÚ PASCUAL, Fernando A., *Secreto Profesional médico. Normas y Usos,* Comares, Granada, 2005.

VIGUERAS PAREDES, Pablo, “La Nueva Regulación de la Historia Clínica”, *Revista General de Legislación y Jurisprudencia,* nº 17, julio 2002, en http://premium.vlex.com

VILLAHERMOSA IGLESIAS, “Los servicios de externalización y la protección de datos”, 2002, en http://www.informatica-juridica.com

VILLAR ABAD, Gloria, “La Regulación de las Instrucciones Previas en la Ley 41/2002”, GONZÁLEZ SALINAS, Pedro y LIZARRAGA BONELLI, Emilio (Coords.), *Autonomía del Paciente, Información e Historia Clínica (Estudios sobre la Ley 41/2002, de 14 de noviembre)*, Civitas, Madrid, 2004.

VILLAR GOÑI, Inmaculada, FAEDDA SANZ, Elena, LARA ECHECHIPÍA, Lourdes y ARAMBURU CLEMENTE, Susana, “Conservación y proceso de digitalización de un archivo de historia clínica”, LEÓN SANZ, Pilar (ed.), *La Implantación de los derechos del paciente,* Eunsa, Barañaín, 2004.

VILLAR ROJAS, F. J., “El Nuevo Régimen de Protección de los Datos de Salud”, *Gaceta Sanitaria*, nº 14, 2000.

VILLAVERDE MENÉNDEZ, J., “Protección de Datos Personales, Derecho a ser Informado y Autodeterminación Informativa del Individuo. A Propósito de la STC 254/1993”, *REDC*, nº 41, mayo-agosto 1994;

-“Derecho de oposición”, TRONCOSO REIGADA, Antonio (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas y Thomson-Reuters, Cizur Menor, 2010.

VITALLER BURILLO, J., “Prevención en Salud Laboral”, VVAA, *Prevención en salud laboral,* Editorial Médica Panamericana, Madrid, 2008.

VIZCAÍNO CALDERÓN, Miguel, *Comentarios a la Ley Orgánica de Protección de Datos de Carácter Personal*, Civitas, Madrid, 2001.

VV.AA, *Derecho Administrativo II. Parte Especial (segunda edición actualizada)*, Universitas, Madrid, 1998.

VVAA, *Robo de Identidad y Protección de Datos,* Aranzadi y Thomson Reuters, Cizur Menor, 2010.

WHITE, Robert y JAMES, Barry, *Manual del Outsourcing. Guía completa de externalización de actividades empresariales para ganar competitividad*, Gestión, Barcelona, 2000.

WILSON, Petra; LEITNER, Christine and MOUSALLI, Antoinette, *Mapping the potential of eHealth: empowering the citizen through eHealth tools and services,* presented at the eHealth Conference, Cork-Ireland, 5-6 may 2004, http://www.epractice.eu/

ZABÍA DE LA MATA, Juan, “Principios Generales”, ZABÍA DE LA MATA, Juan (Coord.), *Protección de datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008;

-“Supuestos que legitiman el tratamiento o cesión de los datos”, ZABÍA DE LA MATA, Juan (Coord.), *Protección de datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008;

-“Tratamiento de datos de facturación y tráfico en servicios de comunicación”, ZABÍA DE LA MATA, Juan (Coord.), *Protección de datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008;

-“Revocación del consentimiento”, ZABÍA DE LA MATA, Juan (Coord.), *Protección de datos. Comentarios al Reglamento,* Lex Nova, Valladolid, 2008.

ZAMORA JIMÉNEZ, Ángel José, “Los Ficheros de las Fuerzas y Cuerpos de Seguridad”, TRONCOSO REIGADA, Antonio (Dir.), Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal, Civitas y Thomson-Reuters, Cizur Menor, 2010.

ZOREDA, J.L.; ICHASO, Mº S y CONBIÁN, F, “Modelo de Tarjeta Personal Inteligente para el seguimiento y control sanitario”*, IyS*, nº 1, noviembre 1991, http://www.seis.es/.

ZOREDA, J. L., SÁNCHEZ FREIRE, M; REDONDO FDEZ. REBOLLO, A; SÁNCHEZ REILLO, R y De PEREDA HUELVES, J, *Tarjeta Sanitaria Inteligente: Terminal Autónomo de Urgencias,* Ponencia presentada en el II Congreso Nacional de Informática de la Salud, 17-19 abril 1997