Universidad del País Vasco Euskal Herriko Unibertsitatea
EKONOMIA ETA ENPRESA FAKULTATEA
FACULTAD DE ECONOMÍA Y EMPRESA

GRADO: Derecho

Curso 2023/2024

La protección penal de los datos registrados en la Historia Clínica

Autor/a: Silvia Gallastegui Martínez

Director/a: María Pilar Nicolás Jimenez

Bilbao, a 15 de febrero de 2024

RESUMEN

La historia clínica recoge información confidencial, conteniendo datos de carácter personal y reservado relativos a la salud. Tratándose de una cuestión estrechamente ligada con la intimidad del paciente, la misma queda regulada en la vigente legislación. Con la llegada de la digitalización, se habla de la historia clínica electrónica. A pesar de que la digitalización suponga numerosas ventajas en el proceso asistencial, permite y facilita el acceso a dichos datos a un mayor número de personas, lo cual entraña riesgos. Es por ello que debe existir una justificación para el acceso a dichos datos, como puede ser el diagnóstico o tratamiento en el marco de una relación asistencial entre profesional sanitario y paciente, pues de lo contrario el mismo se consideraría ilícito, y podría resultar de aplicación el delito de descubrimiento y revelación de secretos. El objetivo de este trabajo es analizar la relevancia de esta cuestión, estudiar cuándo un acceso a la historia clínica de un paciente constituye un ilícito penal y revisar cómo están interpretando este asunto los tribunales.

ABSTRACT

The medical history collects confidential and personal information related to health. As it is a matter closely linked to the patient's privacy, it is regulated by current legislation. With the arrival of digitalization, the electronic medical history is found. Although digitalization brings numerous advantages to the healthcare process, it allows and facilitates access to personal information for a greater number of people, which could cause risks. That is why there must be a justification for access to that information, such as diagnosis or treatment in a healthcare relationship between a healthcare professional and patient, otherwise it would be considered illegal, and could be applicable the crime of discovery and disclosure of secrets. The objective of this project is to analyze the relevance of this issue, study when access to a patient's medical history constitutes a criminal offense and review how the courts are interpreting this matter.

PALABRAS CLAVE

Historia Clínica, confidencialidad, intimidad, datos personales, digitalización, acceso ilícito, fichero, base de datos, secreto, autodeterminación informativa, autorización, consentimiento, profesional sanitario, relación asistencial, perjuicio.

KEY WORDS

Medical History, confidentiality, privacy, personal information, digitalization, illicit access, file, database, secret, informative self-determination, authorization, consent, healthcare worker, healthcare relationship, damage.

Índice

1. Introducción

Debido a los grandes avances tecnológicos, las Tecnologías de la Información y de la Comunicación (TICs) pueden ser utilizadas como medios de comisión de delitos. De hecho, teniendo en cuenta el tema objeto de estudio, cabe destacar que las mismas, pese a las numerosas ventajas que proporcionan, facilitan medios de acceso, modificación, captación y divulgación de datos relativos a la intimidad[1]. Estos datos objeto de estudio -datos de la salud- quedan, mayoritariamente, recogidos en la Historia Clínica Médica, la cual ha pasado por un proceso de digitalización, haciéndola aún más accesible a un mayor número de personas.

El tema objeto de estudio "La protección penal de los datos registrados en la Historia Clínica", es de gran interés social y jurídico pues se trata de un materia que afecta al derecho a la intimidad, un derecho constitucional fundamental y al que se le da especial protección en el ámbito penal en el vigente artículo 197, regulado en el título X "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", capítulo I "Del descubrimiento y revelación de secretos" de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

La protección de datos de carácter personal tiene como fin garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, recogidos en la Constitución Española, así como su honor, intimidad e integridad personal y familiar.

En este sentido, el artículo 197 recoge, en su apartado primero, varias conductas que, en general, afectan al derecho de la intimidad de las personas, considerando tal vulneración como delito cuando se descubran secretos o se vulnere la intimidad de otro sin su consentimiento mediante la apropiación de papeles, cartas, correos electrónicos u otros documentos, así como la interceptación de telecomunicaciones y uso de aparatos de escucha, grabación o difusión de imágenes o sonido.

Es, concretamente, objeto de estudio el apartado 2 del mencionado precepto; supuestos en los cuales, en su perjuicio y sin su autorización, los bienes jurídicos de

---

[1] Antonio Zárate Conde, "La tutela penal de los datos de carácter personal. Una perspectiva jurisprudencial", p. 1, *Diario La Ley*, nº 9422, (2019). Url: https://laleydigital-tutela-penal

terceros y del titular de los datos, se vean vulnerados mediante el apoderamiento, utilización y modificación de datos reservados de carácter personal o familiar que se encuentren registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Así como aquel supuesto en el que se acceda sin autorización a datos contenidos en un sistema informático, y se alteren o utilicen en perjuicio del titular de los datos o de un tercero.

Se pretende mediante este trabajo analizar aquellos supuestos en los que, concretamente, personal sanitario acceda a ficheros electrónicos y obtenga, utilice o modifique datos registrados de carácter personal de pacientes, o familiares, en su perjuicio.

En este sentido, se expondrá, en primer lugar, tanto el contenido como la finalidad de la Historia Clínica, la cual ha sido digitalizada, siendo necesario conocer la legislación que la protege. Además, teniendo en cuenta los supuestos que se analizan en el trabajo, es preciso aclarar quién queda legitimado a su acceso y las situaciones que lo justifican. Se expone, por tanto, cómo queda protegida jurídico-penalmente la Historia Clínica en el ordenamiento jurídico, resaltando el secreto profesional regulado en el artículo 199.2 del Código Penal y la protección de ficheros del artículo 197.2 del Código Penal, centrando el estudio en los elementos de este último delito. Por último, se expone un análisis jurisprudencial estudiando los elementos del tipo y analizando supuestos tipificados como delito del artículo 197.2 del Código Penal, así como la fundamentación jurídica expuesta por los tribunales permitiendo clasificarlos como tal.

2. Datos registrados en la Historia Clínica

2.1. Contenido de la Historia Clínica

2.1.1. Datos de carácter personal

La propia Carta de los Derechos Fundamentales de la Unión Europea, la cual resulta esencial en el desarrollo de un sistema europeo de protección de derechos[2], hace mención, en su artículo 8, a la protección de datos de carácter personal, señalando que

[2] Daniel Jove Villares, *La protección de lo sensible, o cuando la naturaleza del dato no lo es todo,* pp. 91-92, Valencia: Tirant lo blanch, 2023.

"toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan".

Es necesario recalcar que todo aquello que queda recogido en la historia clínica del paciente son, en definitiva, documentos que guardan datos de carácter personal, relacionados mayoritariamente con la salud de un usuario. Quedan así también incluidos los referidos a su porcentaje de discapacidad y a su información genética.

Asimismo, es preciso resaltar el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD en adelante). A efectos del Reglamento se entiende por datos personales "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona." (art. 4. 1) RGPD).

Este precepto recoge una serie de definiciones entre las que también se encuentra en el apartado 15) la de los datos relativos a la salud, quedando definidos como aquellos "datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud" (art. 4.15) RGPD).[3]

También el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, define, en su artículo 2, los datos de carácter personal, así como los ficheros automatizados.

[3] En su considerando número 35 establece que "Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física (...); todo número, símbolo o dato (...), incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, (...) el historial médico, (...), independientemente de su fuente, (...)."

Asimismo, en el ámbito nacional encontramos la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD en adelante). Esta Ley tiene por objeto tanto "adaptar el ordenamiento jurídico español al RGPD, y completar sus disposiciones" como "garantizar los derechos digitales de la ciudadanía conforme al artículo 18.4 de la Constitución." (art.1 LOPDyGDD). Es en la misma donde se recoge el sistema de garantías y de derechos en materia de protección de datos con un tratamiento específico respecto de los datos de salud.

Los derechos que quedan regulados en el RGPD y a los que está facultado el interesado son el derecho de acceso a los datos personales (art. 15 RGPD), el derecho de rectificación (art. 16 RGPD), el derecho de supresión (art. 17 RGPD), el derecho a la limitación del tratamiento (art. 18 RGPD), el derecho a la portabilidad de los datos (art. 20 RGPD), y el derecho de oposición y decisiones individuales automatizadas (arts. 21 y 22 RGPD).

En este sentido, cabe mencionar el Principio de Autonomía, mediante el cual se permite que el paciente tome determinadas decisiones sobre su historial clínico. Este principio se refiere a los derechos de custodia por parte del centro, de acceso, rectificación, cancelación y oposición, y en el derecho del paciente de disponer sobre sus datos de salud.[4]

Teniendo en cuenta el objeto de este trabajo, se estudiará más adelante el derecho de acceso a los datos personales, analizando lo regulado en la LOPDyGDD, así como en la normativa sectorial.

2.1.2. Datos personales de carácter sensibles

A pesar de que, tal y como se indica en el considerando 51 del RGPD, algunos datos personales son, por naturaleza, particularmente sensibles ya que "el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales", no todo dato de salud es sensible ya que cualquier dato de salud no afecta

[4] Juan Pedro Baños Jiménez et al., *Manual de la Relación Médico-Paciente*. (Foro de la Profesión Médica de España, 2019), p. 193. Url: https://manual-relacion-medico-paciente.pdf

de igual manera a los derechos del sujeto.[5] Esto es, no tienen el mismo impacto, ni suponen el mismo riesgo para los bienes jurídicos del sujeto afectado. Es por ello que en función de la naturaleza de la información, exista una mayor o menor peligrosidad.[6]

En este sentido, la historia clínica médica recoge una serie de documentos clínicos que incluyen datos de carácter personal del paciente, datos sensibles, y que merecen especial protección; protección que va en mayor aumento dado al rápido avance tecnológico.

Conforme a la Comisión Europea[7], los datos personales que se consideran sensibles, y que por tanto están sujetos a condiciones de tratamiento específicas son los siguientes:

- datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas,
- la afiliación sindical,
- datos genéticos[8], datos biométricos[9] tratados únicamente para identificar un ser humano,
- datos relativos a la salud,
- datos relativos a la vida sexual u orientación sexual de una persona.

El RGPD dedica una mayor atención a los datos personales relativos a la salud, tanto respecto a su tratamiento con fines asistenciales como de investigación biomédica, incluyendo varias referencias a los datos genéticos. De hecho, los datos personales relativos a la salud, genéticos y biométricos, gozan de una protección más intensa.[10]

---

[5] Pilar Nicolás Jiménez, "El concepto de dato médico y genético", en *Estudios de protección de datos de carácter personal en el ámbito de la salud*, ed. por Santiago Ripol Carulla y coord. por Jordi Bacaria Martrus (Barcelona: Marcial Pons, 2006), pp. 77-101.

[6] Daniel Jove Villares, "*La protección de lo sensible…"* cit. p. 313.

[7] ¿Qué datos personales se consideran sensibles? - Web oficial de la Unión Europea. Url: https://webUE

[8] Definidos en el RGPD (art.4.13)) como aquellos "datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona."

[9] Definidos en el RGPD (art.4.14)) como aquellos "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."

[10] Carlos María Romeo Casabona, "La protección de datos personales en la Unión Europea. Aspectos sectoriales relacionados con la salud", en *Derecho Penal, ciberseguridad, ciberdelitos*

En este sentido, han de atenderse los artículos 4 y 9 del RGPD. El primero de ellos recoge una serie de definiciones entre las que se encuentran las de datos genéticos, datos biométricos y datos relativos a la salud; definiciones que ya han sido expuestas.

Por su parte, el artículo 9.1 RGPD señala que "quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud (...)" salvo que concurra alguna de las circunstancias del apartado segundo de dicho precepto; excepciones relacionadas con el consentimiento del interesado, la protección de intereses del interesado, la anterior publicidad de tales datos por parte del interesado, por razones de interés público esencial, para fines médicos, etc.

Por otro lado, en el ámbito sanitario encontramos también la Ley General de Sanidad, de 25 de abril de 1986 (LGS en adelante) con la que surgió la obligación de registrar la información clínica y que ha sido completada posteriormente por la aprobación de 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 (en adelante, LAP).

Merece especial atención esta segunda (LAP), una norma de regulación sectorial que regula los derechos de autonomía del paciente y el tratamiento de la información clínica y su protección, y donde queda regulada la historia clínica.

A efectos de esta Ley se entiende por Historia Clínica aquel "conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial." (art. 3 LAP).

La historia clínica de un paciente se rige también por el principio de calidad, que protege la confidencialidad de la información clínica, evitando, como aclara TRONCOSO, que se traten datos excesivos en relación con una finalidad concreta.[11] Este

e inteligencia artificial, vol. II: Inteligencia artificial y responsabilidad penal, dir. por Carlos María Romeo Casabona y edit. por Mª Ángeles Rueda Martín (Granada: Editorial Comares, 2023), pp. 3-26.

[11] Antonio Troncoso Reigada, "La confidencialidad de la historia clínica", *Cuadernos de Derecho Público*, nº 27, 2006, p. 68. Url: https://confidencialidad-historia-clínica

principio exige la plenitud y exactitud de la información clínica, el cual se incumple si la historia clínica no es completa, es decir, si no contiene todos los documentos con los datos, valoraciones e informaciones sobre la situación y la evolución clínica de un paciente durante el proceso asistencial.[12] Por ello, el art. 14.1 LAP señala que la historia clínica de cada paciente "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."

El artículo 15.1 LAP hace referencia al contenido de la historia clínica de cada paciente, señalando que esta debe incorporar toda aquella información considerada relevante para el auténtico y actualizado conocimiento del estado de salud del paciente. De hecho, queda recogido en el apartado segundo del mismo el contenido mínimo de la historia clínica, integrada por aquellos documentos que se originan durante el proceso asistencial.

En definitiva, podemos definir la historia clínica como aquel "conjunto de información, único por cada paciente en cada institución asistencial, que se redacta obligatoriamente por los médicos, en el que en beneficio del paciente se reúne la máxima integración de la información a él relativa, al que únicamente tienen acceso el paciente, los facultativos que intervengan en el tratamiento y las personas señaladas por la Ley para fines de inspección sanitaria, científicos o docentes, como expresión de los derechos a la intimidad personal y familiar, y de las obligaciones de confidencialidad y secreto profesional por parte de todos los que tengan acceso a la misma, y en el que deben constar los datos fundamentales de la relación médico-paciente: consentimiento, información y curso de la relación".[13]

[12] Antonio Troncoso Reigada, *"La confidencialidad de la historia clínica"*, cit. p. 71.

[13] Manuel Aulló Chaves y Santiago Pelayo Pardos, "La Historia Clínica", nº1 del Plan de Formación en Responsabilidad Legal Profesional, (Coordinador General: Ricardo De Lorenzo y Montero), Asociación Española de Derecho Sanitario. Edicomplet; Citado por: Luis Pedro Gracieta Royo y Nuria Ibarra García, "La confidencialidad de la historia clínica: una aportación desde la perspectiva del contrato de seguro.", p. 3, *Diario La Ley*, 2000. Url: https://laleydigital-confidencialidad

2.2. Finalidad y legitimación de acceso

2.2.1. Finalidad de la Historia Clínica

La historia clínica médica (HCM) es de gran importancia, teniendo una función puramente asistencial y desempeñando un papel fundamental en la calidad de la atención médica. Sirviendo como documento médico legal, los profesionales sanitarios son capaces de dar con un diagnóstico preciso, evitando errores y conocer todas las características clínicas del paciente y su evolución periódica[14]; lo cual mejora la calidad de los servicios a prestar. Por lo tanto, constituye la herramienta básica en el proceder del diagnóstico.[15]

Cabe añadir que en este proceso asistencial es necesario tener en cuenta la información que proporciona la anamnesis clínica.[16] De hecho, esta información también debe ser registrada en la historia clínica médica, que resulta útil para la investigación clínica y epidemiológica, la docencia, la formación, el Servicio Jurídico Legal, para la realización de estadísticas y para la planificación y gestión de recursos asistenciales.[17]

Por lo tanto, sirve tanto para el diagnóstico y tratamientos médicos, como para la gestión de los servicios sanitarios, así como, fundamentalmente, para garantizar una asistencia sanitaria adecuada al paciente, teniendo acceso a la misma los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente (art. 16.1 LAP). En definitiva, tiene como fin principal "facilitar la asistencia sanitaria, dejando constancia de todos aquellos datos que, bajo criterio médico, permitan el conocimiento veraz y actualizado del estado de salud." (art. 15.2 LAP)

En relación a los datos de la historia clínica, son tres principios genéricos los que han de ser tenidos en consideración, principios aplicables a toda documentación clínica:

---

[14] Raidel González Rodríguez y Juan Cardentey García, *La historia clínica médica como documento médico legal.* Revista Médica Electrónica.vol.37 nº6 Matanzas (2015), ISSN 1684-1824. Url: http://scielo.sld.cu/scielo.hc_documento_médico_legal

[15] Dr. Joan Miquel Nolla, "La importancia de la Historia Clínica", en *El dolor en las enfermedades reumáticas,* (España: Editorial Aresta SC, 2008), pp. 35-39.

[16] Entendida como el procedimiento de exploración que se realiza durante la primera toma de contacto con el objetivo de identificar al paciente, averiguar sus dolencias actuales, su historial y aquellas cuestiones ambientales, familiares y personales más destacables. Ciencias de la Salud,"La anamnesis clínica: objetivos y procedimientos de elaboración.", UNIR - La Universidad en internet, 2021. Url: https://www.unir.net/salud/revista/anamnesis-clinica/

[17] Mercedes Tejero Álvarez, *Documentación clínica y archivo*, 1.ª ed. (Madrid: Diaz de Santos, 2003), p. 9.

Principio de Vinculación Asistencial, Principio de Proporcionalidad y Principio de Autonomía.

El propósito de la propia historia clínica queda justificado en el primero de ellos, en el Principio de Vinculación Asistencial. De hecho, el acceso a la historia clínica queda motivado por la finalidad asistencial, y consecuentemente, también la legitimidad del acceso a la misma por parte de los profesionales sanitarios que intervienen en el proceso asistencial.[18]

El artículo 16.1 LAP indica que "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". Por tanto, cabe afirmar que la finalidad del principio de vinculación asistencial, que legitima el acceso a los profesionales sanitarios y al personal con funciones de inspección, evaluación, acreditación y planificación, administrativas y de gestión[19], es la principal y primera causa justificativa del acceso a la historia clínica.[20]

Por su parte, también el principio de proporcionalidad limita el acceso a la finalidad para la que se obtienen los datos y el uso que de ellos se puede hacer.[21] En otras palabras, en cada momento y situación, el profesional debe acceder únicamente a los datos mínimos necesarios para prestar la asistencia sanitaria concreta.[22]

Por último, por el Principio de Autonomía se faculta al paciente para la toma de ciertas decisiones relativas a su historial clínico; siendo por tanto, interesante destacar sus derechos sobre la misma; principalmente el derecho de acceso.

La obtención de datos masivos de los pacientes relevantes para su salud, provoca una acumulación en los centros sanitarios, de gran cantidad de información que ha de ser tratada y gestionada. Es por ello que los centros tienen la obligación de almacenar la

[18] Juan Pedro Baños Jiménez et al., cit. pp. 193-194.
[19] Juan Luis Beltrán Aguirre, Fernando José García López y Carmen Navarro Sánchez, *Protección de Datos Personales y Secreto Profesional en el ámbito de la Salud: Una propuesta normativa de adaptación al RGPD*, p. 97, (Barcelona: Sociedad Española de Salud Pública y Administración Sanitaria, 2017). Url: https://SESPAS_proteccion_datos_2017.pdf
[20] Andrea Salud Casanova Asencio. *Protección de datos en el ámbito de la historia clínica el acceso indebido por el personal sanitario y sus consecuencias.* (Barcelona: Indret, 2019), p. 6. Url: https://indret.com/2019/07/1463.pdf
[21] Juan Luis Beltrán Aguirre, Fernando José García López y Carmen Navarro Sánchez, cit. p. 97.
[22] Andrea Salud Casanova Asencio., cit. p. 7.

misma con cautela,[23] ya sea en soporte de papel, audiovisual, informático o de otro tipo, con el objetivo de garantizar su seguridad, su correcta conservación y la recuperación de la información (art. 14.2 LAP).

2.2.2. Legitimación de acceso a la Historia Clínica y su custodia

La pérdida o destrucción de algún documento clínico podría afectar gravemente la atención sanitaria. Por lo que la seguridad e integridad de la Historia Clínica, que contiene datos de salud vinculados a la intimidad personal y familiar, resulta esencial. Una de las principales medidas para preservar la misma en el ámbito sanitario es limitar el número de personas que pueden acceder a la historia clínica, estableciendo las adecuadas medidas de seguridad que eviten los accesos no autorizados.[24] Es por ello que, con el fin de conocer quién está legitimado para acceder a la HCM, es necesario estudiar el derecho de acceso a la misma, siendo este derecho de acceso la facultad más relevante con la que cuenta el titular de los datos de carácter personal[25] ya que en el ámbito sanitario, y considerando tanto la numerosa doctrina que ha analizado el derecho de acceso del paciente a su historia clínica como el derecho a la autodeterminación informativa, el acceso permite al titular de los datos de carácter personal controlar lo que sucede con sus datos. Asimismo, en relación con el derecho a la protección de la salud, el acceso le permite conocer cuál es su estado de salud y tomar las decisiones oportunas.[26]

En virtud del artículo 13.1 LOPDyGDD el derecho de acceso "se ejercitará de acuerdo con lo establecido en el artículo 15 RGPD" que señala que el interesado tiene derecho a conocer si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los mismos y a cierta información; información que queda recogida en el apartado primero del mencionado precepto de las letras a) a la h).

---

[23] Carlos María Romeo Casabona, *"La protección de datos personales…"*, cit. pp. 3-26.
[24] Antonio Troncoso Reigada, *"La confidencialidad de la historia clínica"*, cit. pp. 81-82.
[25] Antonio Troncoso Reigada y Juan José González Rivas, "Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales", *Thomson Reuters Aranzadi*, 2021, ISBN: 978-84-1346-416-9. Citado por: Unai Aberasturi Gorriño, cit. p. 675.
[26] Pablo Lucas Murillo de la Cueva, "El derecho fundamental a la protección de los datos relativos a la salud", en *Estudios de protección de datos de carácter personal en el ámbito de la salud*, pp. 21-43, ed. por Santiago Ripol Carulla y coord. por Jordi Bacaria Martrus (Barcelona: Marcial Pons, 2006).

A su vez, la normativa sectorial regula este derecho de acceso del paciente a sus datos personales, así como otros de los derechos mencionados. De acuerdo con el artículo 18.1 LAP, "el paciente tiene el derecho de acceso (...) a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella". En virtud del art. 18.3 LAP el derecho de acceso de los pacientes a 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." Estas anotaciones subjetivas hacen referencia a aquellas valoraciones o impresiones, personales y no objetivas, que el profesional sanitario se forma tras la atención prestada a sus pacientes[27], y que introduce en la historia clínica del paciente. Conforme al art. 19.5 del Código de Deontología Médica, aprobado en julio de 2011 por el Consejo General de Colegios Oficiales de Médicos, establece que esas anotaciones "son de su exclusiva propiedad."

En definitiva, con el fin de prestar la adecuada atención sanitaria, los profesionales sanitarios del centro que realizan el diagnóstico o el tratamiento del paciente deben tener acceso a la historia clínica, derecho que queda expresamente recogido en el art. 16.1 LAP. Por lo tanto, los profesionales sanitarios que no presten o que hayan dejado de prestar atención sanitaria a un paciente no deben acceder a su historia clínica[28], pues de lo contrario, nos encontraríamos ante una conducta delictiva.

Por otro lado, se plantea una cuestión acerca de la titularidad de las historias clínicas[29], habiendo siendo la misma objeto de discusión. La principal razón de este debate radica en los diversos derechos, intereses y obligaciones que surgen en la documentación clínica. En este sentido, se duda sobre quién es el titular de la historia clínica; el paciente, el profesional sanitario o el centro de salud.

De acuerdo con la Ley 41/2002 y el art. 19.2 del Código de Deontología Médica, el paciente tiene el derecho a que se elabore y conserve su historia clínica, donde quedan recogidos los datos personales referidos a su persona. Por tanto, para un sector doctrinal el titular de la documentación médica es el paciente.

---

[27] Pablo Lucas Murillo de la Cueva, *"El derecho fundamental…"*, cit. pp. 21-43.
[28] Antonio Troncoso Reigada, *"La confidencialidad de la historia clínica"*, cit. pp. 101-102.
[29] Laura Salazar Martínez. "La custodia de las historias clínicas". *Diario La Ley*, nº 7951, 2012, pp. 1-6. Url: https://laleydigital-custodia-historia-clínica

No obstante, la custodia de la historia clínica no corresponde al paciente, quien tiene derecho a su acceso[30] limitado y a obtener una copia de la misma (art.18 LAP). Es por ello que para otro sector doctrinal el titular de la historia clínica es el médico o profesional sanitario que la elabora. En este sentido, y como en la historia clínica de cada paciente encontramos una serie de documentos clínicos, la titularidad de la historia clínica quedaría dividida según quien fuera el autor de cada documento.

Por otro lado, otro sector doctrinal considera al propio centro sanitario en el que el paciente es atendido como titular de las historias clínicas ya que corresponde a los mismos la obligación de archivo, elaboración, custodia y conservación de las historias clínicas (arts. 14, 16 y 17 LAP).

Para resolver esta cuestión es necesario destacar la sentencia de la Audiencia Provincial de Pontevedra, de 23 de julio de 2010[31] que indica que "sólo en sentido figurado o impropio cabe hablar de "propiedad" de las historias clínicas. Cuando nos referimos a la propiedad de la historia clínica, estamos, en última instancia, tratando de decidir y determinar a quién corresponde su posesión y custodia (...)" Asimismo, aclaró que "en el caso de médico que ejerce la medicina con la plena autonomía de su consulta particular, a él corresponde la "propiedad" de la historia clínica y, por ende, su conservación y custodia. Si se trata de facultativo que presta sus servicios por cuenta ajena, por ejemplo, de un centro o institución, (...), la historia clínica pertenece al centro donde el profesional presta sus servicios; (..)."[32]

Por lo tanto, tan solo encontramos un supuesto en el que la custodia de la historia clínica no corresponda al centro o institución sanitario; el caso del ejercicio individual de la medicina. De hecho, según lo establecido en el art. 17.5 LAP "los profesionales

[30] Derecho recogido también en el considerando 63 del RGPD cuando señala que "Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud (...)."
[31] Se plantea el caso de varios ginecólogos que prestaban sus servicios en una clínica, de forma autónoma e independiente. Uno de ellos, se llevó consigo las historias de sus pacientes para prestar sus servicios en otra clínica. Aunque actuaba como profesional libre, no lo hacía en condiciones de plena autonomía, sino en la modalidad de medicina colectiva, formando parte de un colectivo profesional y desarrollando así su actividad de forma coordinada. Por lo tanto, la posesión y custodia de las historias clínicas correspondía a la clínica.
[32] Laura Salazar Martínez, cit. p. 5.

sanitarios que desarrollen su actividad de manera individual son responsables de la gestión y de la custodia de la documentación asistencial que generen."

En definitiva, se debe entender la titularidad de la historia clínica en sentido figurado, pues realmente se trata de una legitimidad de acceso y custodia.

2.3. Historia clínica electrónica

Debido al avance de las tecnologías digitales, las relaciones tanto en el ámbito personal como profesional, se han visto modificadas, habiéndose incorporado estas prácticamente a todos los ámbitos de la vida, sin ser los centros sanitarios una excepción.[33]

El anterior sistema por el que se guardaba el historial clínico de cada paciente en formato de papel dificultaba la asistencia y gestión sanitaria ya que las historias clínicas en formato de papel resultaban ser voluminosas, pudiendo llegar a deteriorarse y a ser alteradas, confusas y desordenadas.[34]

Con el fin de ofrecer un servicio de calidad, se hace imprescindible la implantación de un sistema de información que posibilite el tratamiento fácil y seguro de la información sanitaria debido al gran volumen de datos a manipular y la agilidad.[35] Por lo tanto, pudiendo recaer la recogida y tratamiento de datos relacionados con la salud sobre una cantidad masiva de información, se hace necesario un registro o archivo informático que contribuya a dicha gestión.[36] De modo que es necesaria la informatización del sistema.[37]

---

[33] Unai Aberasturi Gorriño, "Los principios de la protección de datos aplicados en la sanidad", Tesis doctoral, Servicio Editorial de la Universidad del País Vasco, 2011, p. 51. Url: https://addi.ehu.es/ABERASTURI.pdf

[34] Mercedes Tejero Álvarez, cit. pp. 7-9.

[35] Noelia De Miguel Sánchez, "Secreto Médico, Confidencialidad e Información Sanitaria", *Marcial Pons*, Madrid, 2003, p. 260. Citado por: Unai Aberasturi Gorriño, cit. pp. 52-53.

[36] Carlos María Romeo Casabona, *"La protección de datos personales…",* cit. pp. 3-26.

[37] Juan Méjica Gracía, "El Enfermo Transparente. Futuro Jurídico de la Historia Clínica Electrónica", *Edisofer*, Madrid, 2002, p. 15. Citado por: Unai Aberasturi Gorriño, cit. pp. 52-53.

Es por ello que surge la idea de la digitalización de las historias en ficheros electrónicos,[38] apareciendo la historia clínica única de salud y centralizada (HCC) y junto a ella una serie de aplicaciones.[39]

La digitalización del historial clínico es el proceso a través del cual la historia clínica de cada paciente es transformada de un soporte en papel a uno digital, quedando superado el anterior sistema de documentación en formato papel.

La Historia Clínica electrónica, siendo el registro en formato electrónico de la información relacionada con la salud de cada paciente que facilita la toma de decisiones por parte de los profesionales de la salud y el tratamiento sanitario[40] permite que la información relacionada con el historial clínico del paciente se encuentre centralizada, actualizada y sea accesible, así como evitar su pérdida, olvido o deterioro físico y facilitar la consulta y control del estado de salud del paciente, de forma sencilla, segura y rápida.[41].

La historia clínica en papel complica la disponibilidad y accesibilidad entre los diferentes niveles de atención[42]. Por lo que la mayor ventaja que trae consigo la Historia Clínica Electrónica es la accesibilidad, facilitando la relaciones entre profesionales, ya que permite las interconsultas entre centros de atención primaria y hospitalaria.[43] Permite la integración de todos los niveles asistenciales y áreas de atención en el proceso asistencial, mejorando las vías de comunicación y la asistencia sanitaria, ya que posibilita una relación continuada, directa y ágil entre profesionales y pacientes, así como entre los propios profesionales sanitarios.[44]

En este sentido, la historia clínica electrónica facilita el establecimiento de distintos niveles de acceso a la misma, permitiendo acceder a todos los datos en ella

---

[38] J.M Ramos-López, M. Cuchí Alfaro y M.A Sánchez Molano, *"Archivo de historias clínicas Digitalizado, una solución previa a la Historia Clínica Electrónica"* (pág 3), Papeles médicos, vol. 18, Núm. 2 (2009). Url: https://papelesmédico-archivohcdigitalizada

[39] Juan Pedro Baños Jiménez et al., cit. p. 195.

[40] Sandra Ferrer Gelabert, "E-salud: La tecnología al servicio de la salud", en *E- salud, autonomía y datos clínicos: Un nuevo paradigma,* dir. y coord. por Cristina Gil Membrado (Madrid: Dykinson, 2021), pp. 13-31.

[41] J.M Portolés y V. Castilla, "Desarrollo y utilización de la historia clínica en soporte electrónico: experiencia de un servicio de nefrología de nueva creación." Nefrología, nº 6, (2002), p. 512-521. Url: https://hc-soporte-electrónico

[42] Ricard Sacartés Fortuny, "Historia clínica electrónica en un departamento de obstetricia, ginecología y reproducción: desarrollo e implementación. Factores clave", p. 12, (Tesis doctoral, Universitat Autònoma de Barcelona, 2013). Url: https://historiaclínicaelectrónica/tesis/2013.pdf

[43] Sandra Ferrer Gelabert, "E-salud: La tecnología al servicio de la salud", cit. pp. 13-31.

[44] Unai Aberasturi Gorriño, cit. p. 60.

contenidos a los profesionales sanitarios autorizados y sólo a aquellos datos relacionados con sus propias funciones al personal de administración y gestión de los centros sanitarios.[45]

Por lo tanto, la información del paciente, independientemente del formato y fuente de la que provengan, se incorpora a una sola base de datos, a la Historia de Clínica Electrónica,[46] la cual facilita el registro de la información clínica[47], la gestión de resultados de pruebas complementarias, las prescripciones y procedimientos y la elaboración de informes,[48] siendo, por tanto, numerosas las ventajas que se presentan. Por este sistema se evitan duplicidades e información dispersa relativas a un paciente que haya pasado por distintos centros, facilitando así, el control y el acceso a la información contenida en la Historia Clínica, contando con una información completa, clara, actualizada y fácil de interpretar.[49]

Además, el mantenimiento de las historias clínicas mediante un sistema informático, que permite la implementación de medidas de seguridad, garantiza la conservación y la confidencialidad de la información. De hecho, facilita la adopción de medidas como el control y restricción de acceso a los datos de los pacientes exclusivamente a los profesionales sanitarios que forman parte del proceso asistencial, cumpliendo así con la seguridad de los tratamientos exigida por la normativa.[50]

A pesar del progreso que todo ello supone, el almacenamiento masivo centralizado de la información clínica entraña, especialmente, grandes riesgos para el secreto y la confidencialidad. De hecho, con la llegada de las nuevas tecnologías, estos peligros y riesgos se han visto multiplicados.[51] Estos potenciales peligros existen debido, precisamente, a la facilidad de realización de copias, transparencia, posibilidades de procesamiento y cruce[52] existentes ya que el número de personas que tiene acceso a sus datos es mayor con este sistema,[53] incluso terceros ajenos. Por lo que, resulta necesaria la

[45] Antonio Troncoso Reigada, *"La confidencialidad de la historia clínica"*, cit. p. 103.
[46] Unai Aberasturi Gorriño, cit. p. 61.
[47] Entendida 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." (art.3 LAP).
[48] Ricard Sacartés Fortuny, cit. p. 14.
[49] Unai Aberasturi Gorriño, cit. p. 62.
[50] Antonio Troncoso Reigada, *"La confidencialidad de la historia clínica"*, cit. p. 84.
[51] Daniel Jove Villares, "*La protección de lo sensible…",* cit. p. 47.
[52] Juan Pedro Baños Jiménez et al, cit. p. 195.
[53] Andrea Salud Casanova Asencio, cit. p. 4.

toma de medidas que eviten un uso irresponsable de los datos, debiendo buscar mayores garantías de seguridad tanto a nivel nacional como internacional.[54]

En definitiva, se pueden plantear nuevos problemas jurídicos y éticos, pudiendo ser las historias clínicas objeto de delito, resultando así vulnerada la intimidad de los pacientes. Es decir, pueden surgir varios inconvenientes en la accesibilidad a los sistemas ya sea desde la complejidad o disponibilidad tecnológica de las personas hasta la vulneración de derechos de los pacientes.[55] Uno de los principales riesgos que puede aparecer, y que es precisamente objeto de estudio en este trabajo, es la facilidad de acceder a ficheros informáticos.[56] Es esta amenaza a la confidencialidad e intimidad la que hace que sea necesario tipificar aquellas conductas que afecten a la misma.[57]

3. La protección jurídico-penal de los archivos informáticos clínicos en el ordenamiento jurídico

3.1. La protección general de la historia clínica en el ordenamiento jurídico

El derecho fundamental a la protección de los datos de carácter personal permite al individuo controlar el acceso por terceros a sus datos personales y al tratamiento que de ellos se hagan o se quieran hacer,[58] siendo necesario encontrar el equilibrio entre la gestión de la salud pública y el respecto a la intimidad y privacidad de los pacientes.[59]

Teniendo en cuenta que los pacientes, como personas que son, tienen el derecho a la gestión libre de sus derechos[60], quedan reconocidos los derechos a la intimidad, al

---

[54] Aitziber Emaldi Cirión, "El ciberespacio como nuevo escenario para vulnerar derechos fundamentales", en *Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial,* vol. II: Ciberseguridad y ciberdelitos, dir. por Carlos María Romeo Casabona y edit. por Mª Ángeles Rueda Martín (Granada: Editorial Comares, 2023), pp. 101-125.
[55] Sandra Ferrer Gelabert, "E-salud: La tecnología al servicio de la salud", cit. pp. 13-31.
[56] Aitziber Emaldi Cirión, cit. pp. 101-125.
[57] Juan Pedro Baños Jiménez et al., cit. p. 195.
[58] Pablo Lucas Murillo de la Cueva, "El derecho fundamental…", cit. pp. 21-43.
[59] Ana Isabel Herrán Ortiz, "Datos personales de salud, investigación científica y tecnología big data. De la necesidad de un marco normativo propio en la UE", en *E- salud, autonomía y datos clínicos: Un nuevo paradigma,* dir. y coord. por Cristina Gil Membrado (Madrid: Dykinson, 2021), pp. 179-216.
[60] Javier Júdez, Pilar Nicolás, M. Teresa Delgado, Pablo Hernando, José Zarco y Silvia Granollers, "La confidencialidad en la práctica clínica: historia clínica y gestión de la información", *Medicina Clínica* 118 (2002): 18–37. DOI:10.1016/S0025-7753(02)72271-9

honor y a la privacidad, así como a la propia imagen, o a la protección de datos personales, existiendo, por tanto, determinadas informaciones o datos conocidos en el ejercicio de la profesión que deben reservarse al acceso y conocimiento de otros.

La ley 41/2002, en su artículo 7, reitera el derecho a la intimidad de los pacientes y garantiza la confidencialidad de los datos referentes a su salud, prohibiendo que se acceda a ellos, sin previa autorización. Además, impone en los centros sanitarios, la obligación de adoptar las medidas necesarias para salvaguardar los derechos de los pacientes.[61]

De modo que, no resultando sencillo delimitar el alcance de lo íntimo o privado, es evidente que los profesionales sanitarios, conocen datos e informaciones relativas a la esfera tanto íntima, privada como pública de las personas; distinguiendo entre lo íntimo y privado, respectivamente, como aquellos datos sensibles que conforman el núcleo duro de la intimidad y aquellos datos no tan sensibles pero de un ámbito de vida particular[62].

La historia clínica refleja la relación entre el paciente y el profesional sanitario, la cual se caracteriza por la existencia de un ambiente de confianza y lealtad[63], conteniendo información de carácter sensible.

Esta relación médico-paciente exige que el paciente tenga pleno conocimiento sobre su estado de salud.[64] Es por ello que la confidencialidad resulta esencial en dicha relación. El paciente, de acuerdo con el principio de autonomía puede revelar los datos que considere oportunos siendo necesario aportar una información veraz y suficiente para la correcta asistencia. Ello implica la cesión por parte del paciente de una parte reservada de sí mismo, de información confidencial[65], a cambio de una adecuada atención. Ante esta revelación de datos, lo cual supone abrir su esfera más íntima, el paciente ha de

[61] Pablo Lucas Murillo de la Cueva, *"El derecho fundamental…"*, cit. pp. 21-43.
[62] Cesáreo García Ortega y Victoria Cózar Murillo, "La intimidad del paciente: novedades legislativas", *Medicina Clínica* 115 (2000): 426-427. DOI:10.1016/S0025-7753(00)71579-X
[63] Javier Júdez, Pilar Nicolás, M. Teresa Delgado, Pablo Hernando, José Zarco y Silvia Granollers, cit. pp. 18-37.
[64] Unai Aberasturi Gorriño, cit. p. 684.
[65] Un dato confidencial es aquel que se conoce en confianza, con seguridad recíproca entre dos o más personas. En el ámbito sanitario toda persona que por su relación laboral conozca información confidencial, ya sea por participar directamente en la asistencia sanitaria del paciente como por ser necesaria su colaboración en dicha asistencia, deben respetar el derecho a la confidencialidad del paciente. (Javier Júdez, Pilar Nicolás, M. Teresa Delgado, Pablo Hernando, José Zarco y Silvia Granollers, cit. pp. 18–37.

confiar en el profesional pues se entiende que existe un contrato tácito que obliga a guardar silencio.[66]

El concepto de confidencialidad supone hablar de unos límites en cuanto a la preservación de las informaciones sensibles compartidas. Cabe destacar que, tal y como se justificará más adelante, toda la información relativa a la salud es considerada como sensible.[67]

Por lo tanto, como la relación de los pacientes con los profesionales de la salud se basa necesariamente en la confianza y es el paciente quien debe revelar datos que pertenecen a su intimidad, y debido a la naturaleza de la información recogida en la Historia Clínica, este documento requiere de una gran protección, resultando necesario para el profesional que la elabora conocer determinados aspectos que la regulan y las consecuencias jurídico-penales a las que se enfrenta si vulnera su protección y su contenido. En este sentido, son varias las normas legales que obligan al secreto profesional.[68]

Partiendo de la vinculación existente entre el secreto[69] médico y el derecho a la intimidad, debemos destacar la Constitución Española, 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, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDyGDD), la Ley 14/1986, de 25 de abril, General de Sanidad (LGS), el art. 199 del Código Penal y los Códigos Deontológicos. Por lo tanto, los profesionales sanitarios tienen la obligación legal, estatutaria y deontológica de confidencialidad y reserva de los datos médicos de los pacientes. Esta obligación no les permite revelar los datos a terceros, datos de los son conocedores por razón de su oficio.[70] De manera que todo aquel que conozca esta

[66] J. Antomás y S. Huarte del Barrio, "Confidencialidad e historia clínica. Consideraciones ético-legales", p. 75, An. Sist. Sanit. Navar, Vol. 34, nº 1 (2011). Url: https://scielo.isciii.es/pdf/asisna/v34n1/revision2.pdf

[67] Javier Júdez, Pilar Nicolás, M. Teresa Delgado, Pablo Hernando, José Zarco y Silvia Granollers, cit. pp. 18–37.

[68] J. Antomás y S. Huarte del Barrio, cit. p. 73.

[69] El secreto hace referencia a aquello que forma parte de la esfera privada de cada persona, de la intimidad, es decir, aquello que es sólo conocido por su titular o por quien éste determine (Sentencia 809/2017, de 11 de diciembre, FJ.4).

[70] Carlos Peñalosa Torné y Lucía Matarredona Chornet,) "El delito de descubrimiento de secretos por el acceso ilícito al historial médico del paciente", p. 1, *Diario La Ley*, nº 10366. Url: https://laleydigital-delito-acceso-ilícito

información en el ejercicio de sus funciones, tiene el deber de guardar el secreto profesional, preservando, y sin poder divulgar, todo dato reservado o secreto, contribuyendo, así, a un ambiente de confianza y lealtad.

Por su parte, en el ámbito sanitario, la Ley General de Sanidad, en el apartado 3 del artículo 10 recoge el derecho del paciente "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".

Asimismo, la LOPDyGDD recoge el deber de confidencialidad en su artículo 5 señalando que los responsables y encargados del tratamiento de datos están sujetos al deber de confidencialidad (art. 5.1) y que esta obligación es complementaria de los deberes de secreto profesional conforme a su normativa aplicable (art. 5.2).

En la legislación civil, desde 1982, se considera intromisión ilegítima en el ámbito de la intimidad "la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela" (art. 7.4 Ley Orgánica 1/1982).

Por su parte, mientras que el Código Penal anterior no castigaba la revelación del secreto profesional como delito específico, la nueva redacción del Código Penal de 1995 incorpora el delito de incumplimiento del deber de confidencialidad (secreto profesional).[71]

Asimismo, queda reconocido el carácter confidencial de los datos y el deber de secreto profesional tanto en el Código de Deontología Médica como en el de Enfermería.[72] Respecto al acceso al historial médico, el artículo 27.3 del Código de Deontología Médica indica que "el hecho de ser médico no autoriza a conocer información confidencial de un paciente con el que no se tenga relación profesional".

Por tanto, la responsabilidad del personal sanitario por incumplimiento del secreto profesional puede ser civil, penal, disciplinaria o deontológica.[73]

[71] Javier Júdez, Pilar Nicolás, M. Teresa Delgado, Pablo Hernando, José Zarco y Silvia Granollers, cit. pp. 18–37.
[72] Carlos Peñalosa Torné y Lucía Matarredona Chornet, cit. p. 1.
[73] Jesús García Garriga, "El acceso indebido a los datos clínicos por personal sanitario y la aplicación de los art. 197 y 198 del CP: aproximación a dos recientes sentencias de hechos

A pesar de que la obligación de secreto profesional es una obligación, fundamentalmente, deontológica, disciplinaria y también penal, la protección de la Historia Clínica no deriva de esta obligación deontológica del secreto profesional sino que deriva de la LOPDyGDD y de lo regulado en el art.197.2 del Código Penal.

En definitiva, teniendo en cuenta que los sujetos tienen unos derechos sobre los datos de carácter personal, la Historia Clínica, y consecuentemente, todos aquellos datos personales de los pacientes contenidos en ella, quedan protegidos por varias vías: la obligación de secreto profesional y la protección de ficheros que contienen los datos de carácter personal. La principal diferencia a destacar radica en que mientras que el deber de secreto profesional existe debido a la relación asistencial entre paciente y profesional sanitario impidiéndole al sanitario la divulgación de la información confidencial conocida gracias a dicha relación, la protección de los ficheros tiene lugar ya que de la obligación de guardar secreto profesional no deriva la prohibición del acceso al historial clínico médico de los pacientes no asignados sino que deriva de la de la obligación de respeto hacia los datos de otro registrados en tales ficheros, existiendo un "deber de autodeterminación informativa".

3.2. La protección penal: El delito de descubrimiento y revelación de secretos

Los delitos de descubrimiento y revelación de secretos se pueden definir como aquellos tipos penales que protegen el derecho a la intimidad, tanto en la vertiente negativa como positiva. Mientras que la primera de ellas se refiere a la exclusión del conocimiento de terceros aquellas cuestiones secretas o reservadas relativas a la vida privada de uno mismo, la segunda se refiere a la reserva a un determinado círculo de personas de determinados aspectos de la vida privada.[74]

Teniendo en cuenta que la salud forma parte de la estricta intimidad de las personas y que la Constitución Española garantiza la intimidad personal y familiar,

idénticos y fallos dispares", pp. 157-158, *Juristas de la salud*, Vol. 25, nº 2 (2015). Url: https://www.accesoindebido-2020-05/vol25n2_07_Estudio.pdf

[74] Julio Vírseda de Andrés, "Los delitos contra la intimidad tras la reforma 1/2015 de 30 de marzo del Código Penal. Especial consideración al delito de sexting", p. 10, (Trabajo de fin de grado, Universidad de Valladolid, 2016). Url: https://lc.cx/dAGojD

quedando reconocido el derecho a la intimidad como derecho fundamental en su artículo 18, los datos de salud gozan de una especial protección.

Es por ello que el delito de descubrimiento y revelación de secretos queda regulado en el Código Penal de 1995, aprobado por la Ley Orgánica 10/1995 de 23 de noviembre, que protege jurídico-penalmente el derecho a la intimidad en su Libro II, Título X, nombrado "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", concretamente, en el Capítulo I "Del descubrimiento y revelación de secretos", entre los artículos 197 y 201 del Código Penal, castigando aquellas conductas con las que se vulnera la intimidad de otra persona o se descubren sus secretos.

Queda, por tanto, regulado en el Código Penal, el deber de secreto, quedando, asimismo, protegido como el deber de autodeterminación informativa ya que la Historia Clínica es, en definitiva, un archivo de datos. De manera que, queda amparada penalmente, vía el artículo 199.2 CP y el art. 197.2 CP, la libertad y la autodeterminación informativa de los pacientes. Es por ello que en este epígrafe es preciso centrar la atención en el ámbito penal y realizar una comparativa entre ambos preceptos.

3.2.1. Bienes jurídicos protegidos

Con el fin de analizar jurídico-penalmente la figura delictiva objeto de estudio, resulta necesario comenzar exponiendo el bien jurídico protegido en el artículo 197.2 y 199.2 del Código Penal.

El bien jurídico protegido en los delitos de descubrimiento y revelación de secretos es la intimidad, en general, siendo esta un derecho fundamental reconocido en la Constitución Española cuando dispone, en el Título I “De los derechos y deberes fundamentales”, concretamente, en el artículo 18 apartado primero y cuarto lo siguiente:

> “1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. (…)
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.”

Según doctrina reiterada del Tribunal Constitucional, el derecho fundamental a la intimidad, que deriva de la dignidad de la persona (art. 10.1 CE), siendo un valor inherente a la misma y que implica la libertad de las personas para elegir su propia vida y obtener el respeto por parte de los demás[75], pretende garantizar el ámbito reservado de la vida privada de los individuos frente al conocimiento de los demás (STC 115/2013 de 9 de mayo).

ROMEO CASABONA entiende por intimidad aquellas manifestaciones de la personalidad individual o familiar, cuyo conocimiento quedan reservados a su titular o sobre las que ejerce control, cuando se ven implicados terceros, ya sean particulares como los poderes públicos. De hecho, no solo queda incluido el conocimiento, sino también el desenvolvimiento o el desarrollo en sí mismo.[76]

De acuerdo con el Tribunal Supremo, "lo que el artículo 18.1 CE garantiza es el secreto sobre nuestra propia esfera de vida personal y, por tanto, veda que sean los terceros, particulares o poderes públicos, quienes decidan cuáles son los contornos de nuestra vida privada" (STS 176/2013, de 21 de octubre, FJ 7).

Por su parte, el apartado 4 de dicho precepto, que conforme a JOVE[77], requeriría de una conveniente reforma con el fin de adaptarlo a la realidad actual teniendo que incorporar de forma clara el derecho a la protección de datos, así como los derechos que engloba como son, el derecho de acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos y oposición, a pesar de que haya ido evolucionando y mostrando su flexibilidad por haber facilitado la incorporación al catálogo de derechos fundamentales el derecho a la protección de datos, alude a la autodeterminación informativa, que en el ámbito sanitario, queda manifestado mediante la facultad de control de los datos de carácter personal, fundamentalmente por el derecho de acceso a la historia clínica (art. 18 LAP), y por la capacidad de decidir sobre las intervenciones médicas.[78]

---

[75] Aitziber Emaldi Cirión, cit. pp. 101-125.
[76] Romeo Casabona, "Derecho penal, Parte especial", En *Comentarios al Código Penal, Vol. II* (España: Tirant lo Blanch, 2004), ISBN:9788484560029, p. 255.
[77] Daniel Jove Villares, "La protección de datos: un derecho para el entorno digital", Juventud y constitución: un estudio de la Constitución española por los jóvenes en su cuarenta aniversario, coord. por Andrés Iván Dueñas Castrillo, Daniel Fernández Cañueto, Gabriel Moreno González, 2018, ISBN 9788494620140, pp. 98-99. Url: https://actas14_juventud_constitucion_dig.pdf
[78] Pilar Nicolás Jiménez, "La protección jurídica de los datos genéticos de carácter personal", p. 240 (Tesis Doctoral, Universidad de Deusto, 2006).

Además, el Tribunal Supremo, en la STS 803/2017, de 11 de diciembre de 2017, (FJ 4), expone que "el derecho a la protección de los datos de carácter personal deriva del artículo 18.4 CE y consagra en sí mismo un derecho o libertad fundamental, que excede el ámbito propio del derecho fundamental a la intimidad (artículo 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona".

La finalidad del derecho a la protección de datos, se basa precisamente en la protección frente a los riesgos derivados del tratamiento de información de una persona. De manera que cuanto más íntima o reservada sea dicha información mayores riesgos se generan; riesgo no es inherente al dato, sino al tratamiento de la información.[79]

En este sentido, y a pesar de que se haya dicho que la intimidad sea el bien jurídico protegido, se debe puntualizar que, concretamente entre el artículo 197.2 CP y el artículo 199.2 CP, existe una diferencia, precisamente, en relación al bien jurídico protegido ya que, como se explicará más adelante, el artículo 197.2 protege la autodeterminación informativa y el artículo 199.2 protege la intimidad (STS 809/2017, de 11 de diciembre). Se incidirá sobre ello cuando se analicen detalladamente los elementos objetivos y subjetivos del tipo principal objeto de estudio de este trabajo, el art. 197.2 CP.

3.2.2. Las conductas

Siendo la conducta descrita en cada uno de los tipos distinta, será aplicable un tipo u otro en función de cuál sea la acción cometida, debiendo, asimismo, tener en cuenta la concurrencia del resto de elementos del tipo.

El artículo 199 CP castiga, en primer lugar, a aquel que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales (art. 199.1 CP) y, en segundo lugar, al profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona (art.199.2 CP). Es, precisamente, este último el que recoge la vulneración del secreto profesional, sancionando la divulgación de los secretos del paciente, lo cual supone una deslealtad para con el mismo.

Por su parte, el artículo 197.2 CP, el cual está dividido en dos incisos, recoge el delito de descubrimiento y revelación de secretos en soporte electrónico, tutelando la

[79] Daniel Jove Villares, "*La protección de lo sensible…"* cit. pp. 325-326.

intimidad informática. Las conductas en él descritas afectan a datos que no están bajo la custodia del titular, sino en bancos de datos (STS 1328/2009, de 30 de diciembre de 2009). De acuerdo con el mismo, será castigado aquel "que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado", así como "a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero." (art. 197.2 CP)

En el epígrafe cuarto de este trabajo se estudiará con mayor detalle los elementos objetivos y subjetivos del artículo 197.2 del Código Penal y se analizarán algunos supuestos.

Por lo tanto, el apartado segundo del artículo 197 CP castiga a aquel que realiza las conductas mencionadas sin estar autorizado y cuando los datos se hallan en un soporte electrónico. En cambio, el artículo 199.2 CP regula la divulgación de secretos tras incumplir con el deber de sigilo. Esta divulgación es entendida como "la acción de comunicar por cualquier medio, sin que se requiera que se realice a una pluralidad de personas toda vez que la lesión al bien jurídico intimidad se produce con independencia del número de personas que tenga el conocimiento" (STS 809/2017, del 11 de diciembre y STS 574/2001, de 4 abril). De hecho, a diferencia de lo que sucede en el artículo 197.2, en el 199.2 no se exige la intención de perjudicar a un tercero, sino simplemente divulgar secretos.[80]

3.2.3. Sujetos activos

El artículo 199.2 del Código Penal contempla el delito de revelación de secretos por parte de profesionales, describiendo, por tanto, un delito especial propio refiriéndose al profesional.[81]

En el ámbito sanitario, los profesionales tienen conocimientos de ciertas informaciones de carácter personal y confidencial. El fundamento del delito se encuentra

[80] Pilar Nicolás Jiménez, *"La protección jurídica de los datos genéticos…",* cit. p. 158.
[81] Pilar Nicolás Jiménez, *"La protección jurídica de los datos genéticos…",* cit. p. 152.

en la obligación de sigilo y secreto del profesional que, por razón de su condición y del servicio prestado, es conocedor de confidencias y datos personales que forman parte de la esfera íntima de terceros, concretamente, en el supuesto que nos ocupa, de la intimidad de los pacientes (STS 809/2017, de 11 de diciembre). De modo que, en el supuesto objeto de estudio, el sujeto pasivo del artículo 199.2 es aquel paciente que deposita la confianza en el profesional y con quien comparte información relativa a su persona.[82]

El Tribunal define el concepto del profesional, señalando que profesional es aquel que "presta un servicio cuyo desempeño va unido al conocimiento de una información necesaria para el cumplimiento de su función y que queda legalmente obligado a no revelar." Añade, además, que "el guardar secreto forma parte necesaria del núcleo central de los servicios propios de la profesión que ejerce." (STS 809/2017, de 11 de diciembre (FJ 4)). De hecho, se conoce a dicho profesional como "confidente necesario"[83], ya que es sabedor de determinadas informaciones por razón de su cargo.

Por lo tanto, a diferencia del sujeto activo del art. 197.2 CP, que puede serlo cualquier persona, el sujeto activo del art.199.2 CP sólo puede serlo el profesional.

No obstante, en el supuesto concreto que nos ocupa, como ambos delitos son cometidos por profesionales sanitarios, debemos hacer hincapié en la diferencia entre el art.197.2 y 199.2 del Código Penal.

Mientras que el primero de ellos hace referencia a aquellos casos en los que el sanitario acceda, utilice o modifique datos de carácter personal en su perjuicio sin estar autorizado para acceder a los ficheros informáticos en los que se encuentran, el segundo alude al secreto sanitario del que está en posesión el personal sanitario. Es decir, aquel supuesto en el que el profesional difunda datos personales del paciente que conozca por existir una relación asistencial entre ellos, esto es, por ser él mismo el profesional que lo atiende o por estar involucrado en el proceso asistencial del paciente. Es precisamente esta condición el elemento típico del artículo 199.2 (STS 809/2017, de 11 de diciembre).

Por lo tanto, en este supuesto regulado en el art.199.2 CP, no se está accediendo a la historia clínica médico del paciente sin permiso, sino por razón de su cargo conoce

[82] Pilar Nicolás Jiménez, *"La protección jurídica de los datos genéticos…"*, cit. p. 156.
[83] Virginia Mayordomo Rodrigo, "Un supuesto de colisión de deberes: la obligación de denunciar y el mantenimiento del secreto profesional", p. 7, *Actualidad Penal*, nº 33 (2002). Url: https://laleydigital-colisión-deberes

los datos recogidos en la misma y los divulga, incumpliendo su obligación de guardar secreto profesional.

3.2.4. Supuesto de aplicación del art. 197.2 CP y art. 199.2 CP

El deber de sigilo del médico no se refiere a todos los secretos del paciente que el sanitario pueda llegar a conocer. En este sentido, todo dato íntimo o personal que le haya sido revelado voluntariamente al sanitario y que sea ajeno a la salud, no se ve protegido por el deber de sigilo del profesional, ya que el art. 199.2 CP se refiere, únicamente, a los datos de la salud conocidos profesionalmente. Es más, para que la intimidad pueda ser considerada lesionada, debe tratarse de datos relativos a la salud que no sean públicamente conocidos por terceros y que tengan cierta entidad.[84]

Por lo tanto, para que resulte aplicable el art. 199.2 CP, se ha de tratar de supuestos en los que los profesionales cuenten con un acceso lícito a la intimidad de terceros, debiendo un deber de sigilo o reserva y que este haya sido incumplido mediante la divulgación de la información secreta.

A pesar de la diferencia entre estos dos preceptos, en muchas ocasiones resultan ambos aplicables. Así, por ejemplo, y con el fin de conocer cuándo resultan aplicables, es preciso analizar la STS 778/2013, de 22 de octubre,[85] por la que se absuelve a un médico que había sido condenado por aplicación del art.197.2 y art.199.2 CP tras difundir datos médicos con el fin de denunciar irregularidades en los implantes mamarios realizados en una clínica sobre múltiples pacientes, a las que se le habían implantado prótesis mamarias de una marca distinta a la que figuraban en la documentación. Es por ello que decidió consultar el historial médico tanto de las pacientes a las que él había intervenido, como el de otras pacientes intervenidas por otros doctores. Tras asesorarse jurídicamente, el médico denunció las irregularidades observadas.

---

[84] Ángeles Jareño Leal, "El secreto profesional del médico. Referencia especial a los pacientes menores de edad". *La ley penal: revista de derecho penal, procesal y penitenciario*, nº 32, (2006), p. 2. Url: https://laleydigital-secreto-profesional

[85] Carlos Prat Westerlindh, "Descubrimiento y revelación de secretos por un médico que denuncia irregularidades en implantes mamarios", *La ley penal: revista de derecho penal, procesal y penitenciario*, nº 107 (2014): 7. ISSN 1697-5758. Url: https://laleydigital-irregularidades-implantes

Ante la difusión de los historiales médicos de los pacientes, el médico fue denunciado en aplicación del art. 197.2 y 199.2 del Código Penal.

El Tribunal de instancia absolvió al médico de un delito de revelación de secretos del art.199 del Código Penal, al considerar que se trataba de un error invencible "porque recabó asesoramiento jurídico por lo que estaba convencido que actuaba dentro de la legalidad" al denunciar los hechos.

Por su parte, la Audiencia Provincial, considerando que actuó bajo un error de prohibición vencible (art. 14 CP) por no haber realizado un estudio previo sobre la peligrosidad de los implantes efectuados, condenó al médico. Frente a ello, se interpuso recurso de casación.

El Tribunal Supremo declara que "en el caso de los historiales de los pacientes respecto a los que el acusado interviene médicamente no hay descubrimiento de secreto en la medida en que el médico que interviene es el que elabora la historia clínica y su contenido no era secreto para él. Por el contrario, aquellos otros historiales en los que el acusado, médico cirujano, no ha intervenido profesionalmente, su contenido sí es secreto y su descubrimiento rellena la tipicidad." Por lo tanto, conforme al Tribunal Supremo, el profesional sanitario que trata a un paciente conoce ya su historia clínica por razón de cargo, estando facultado para su acceso.

El Tribunal Supremo no comparte el argumento de la Audiencia por dos razones. En primer lugar, porque el examen sobre la situación de riesgo generada por los implantes colocados en pacientes debe ser realizado en el momento en que el doctor percibe que no son los implantes que la clínica se comprometió a colocar. En segundo lugar, porque considera que el acusado, siendo médico especialista en cirugía estética, tenía los suficientes conocimientos como para calibrar el riesgo que estas intervenciones médicas pueden generar. En este sentido, el médico valoró el riesgo ante el que se encontraban las pacientes, y actuó pensando en la salud de los pacientes.

Por ello, a pesar de que el médico accediera al historial clínico de varias pacientes sin autorización ni relación asistencial que lo justificara, el Tribunal Supremo consideró que su actuación fue la adecuada. Por ello, y a pesar de que el Tribunal Supremo entiende que el acusado se excedió, no considera suficiente dicho exceso como para generar responsabilidad penal.

En definitiva, el acceso y la difusión pública no autorizada al historial médico puede constituir un delito del art. 197 y un delito del art.199 del Código Penal.

Una vez aclarada la diferencia entre estos artículos y teniendo en cuenta que en este trabajo resulta de interés encajar el delito de descubrimiento y revelación de secretos en el ámbito sanitario y, concretamente, cuando los datos reservados de carácter personal sean obtenidos, en perjuicio de tercero, de ficheros o soportes informáticos, o cualquier otro tipo de archivo o registro, se realiza, en el próximo epígrafe, un análisis profundo sobre el art.197.2 CP en aplicación al supuesto objeto de estudio, en el que sin vulnerar ninguna medida de seguridad por tener acceso facilitado por razón de oficio a los soportes electrónicos y demás programas, vulneran la intimidad del paciente por acceder a sus datos de carácter personal sin estar autorizados para acceder a los mismos.

4. Proyección de los elementos del art. 197.2 a este supuesto concreto

El tipo del injusto tiene una vertiente objetiva, compuesto por todos los elementos de naturaleza objetiva que caracterizan el supuesto de hecho de la norma penal; y una vertiente subjetiva, compuesta por el contenido de la voluntad que rige la conducta delictiva.

Teniendo en cuenta los diversos apartados del artículo 197 CP, es sencillo comprender y estar de acuerdo con lo señalado por la doctrina, que ha calificado el artículo 197 CP como un "auténtico galimatías jurídico con diabólica, atormentada e inacabable redacción" (STS 412/2020, de 20 de julio de 2020, ECLI: ES:TS:2020:2736). Es por ello, que, con el fin de clarificar la tipicidad del artículo 197 del Código Penal, el TS señala que en él se regulan diversos tipos básicos, así como varias figuras agravadas, quedando tipificados, en los dos primeros apartados, una serie de comportamientos.

El tipo básico queda regulado en los apartados 1 y 2 del artículo 197 del Código Penal. De hecho, MARTÍN-CASALLO LÓPEZ[86] entiende que sólo tienen sustantividad

[86] Martín-Casallo López, "Problemática jurídica en torno al fenómeno de Internet", en *Cuadernos de Derecho Judicial,* CGPJ, Madrid, 2000, p. 21; Citado por: Antonio Abellán Albertos, "Protección penal de los datos de carácter personal y de los programas informáticos", p. 5, *Diario La Ley Penal*, nº 5811, (2003): 1750-1769. Url: https://laleydigital-protecciónpenaldatos

propia estos dos primeros apartados, necesitando el resto de apartados ser complementados con los dos primeros, siendo supuestos que agravan la pena, por ejemplo, dependiendo de la cualificación del sujeto activo, del tipo de datos que resulten afectados o de los fines con los que se cometen los hechos.

A pesar de que el tipo objeto de estudio sea el artículo 197.2 del Código Penal en proyección al supuesto de que sea el personal sanitario el sujeto activo, procede realizar una breve diferencia entre los dos primeros apartados del artículo 197 CP.

Cabe destacar que ambos son un delito común que puede ser cometido por cualquier persona, es decir, el autor no debe reunir una serie de condiciones.

El primer apartado castiga a aquel que "para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación."

Junto con el dolo, se exige que se realice alguna de las conductas mencionadas, exigiendo, por tanto, un elemento subjetivo de lo injusto que se pone de manifiesto con la empleada preposición "para". Por lo tanto, se trata de un delito de intención y de resultado cortado que consiste en la realización de un acto con el fin de que se produzca un resultado determinado,[87] así como de un tipo mixto alternativo[88] que puede consumarse de dos maneras, bien mediante el apoderamiento de documentos y de efectos personales o mediante la interceptación de telecomunicaciones.

Centrándonos ahora en el segundo apartado del artículo 197 CP, cabe destacar que, tal y como resalta la jurisprudencia, el art.197.2 CP describe el tipo básico de los delitos contra la libertad informática o habeas data, así denominados por la doctrina, persiguiendo el legislador los abusos informáticos contra la intimidad de las personas.[89]

---

[87] Mª Ángeles Rueda Martín, *La nueva protección de la vida privada y de los sistemas de informatización en el Código Penal*, Barcelona: Atelier, 2018, pp. 91-92.
[88] Pilar Otero González, "Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio", en *Memento Práctico Francis Lefebvre. Penal Económico y de la Empresa,* Madrid, 2011.
[89] Javier Zaldívar Robles, "La protección penal del derecho a la intimidad", *Teorder*, nº 19, 2016, p. 175.

Se trata de delitos que atentan contra la intimidad de las personas haciendo un uso ilegítimo de los datos personales insertados en un programa informático.[90]

En un primer momento, el Proyecto de 1994 solamente decía que "las mismas penas se impondrán al que, sin estar autorizado, se apoderase de datos reservados de carácter personal o familiar de otro, registrados en ficheros, soportes informáticos o cualquier otro tipo de archivo o registro, público o privado" (art. 188.2). No obstante, la redacción actual es algo más compleja, llegando a resultar confusa incluso para la doctrina. De hecho, las diversas alternativas que se describen en el tipo del art. 197.2 CP, no ayuda excesivamente a su clarificación, debido a los incisos que recoge su descripción (STS 412/2020 de 20 de Julio de 2020). En este sentido, MARTÍN-CASALLO opina que, siendo la acción similar en ambos, no resulta sencillo precisar cuáles son sus elementos diferenciadores[91].

Para poder analizar, en primer lugar, los elementos objetivos del injusto es necesario aclarar que el actual artículo 197.2 CP señala lo siguiente:

> "Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero."

Como se ha explicado, así como la libertad informática reconocida en el apartado 4 del artículo 18 CE, el derecho a la intimidad personal es un derecho fundamental, reconocido en el apartado primero, que deriva de la dignidad de la persona (art. 10.1 CE).

[90] Francisco Soto Nieto, "Revelación de secretos. Entidad del dato revelado", p. 1, *Diario La Ley*, nº 6132, (2004). Url: https://laleydigital-laleynext-entidad-dato

[91] Martin-Casallo López, "Problemática jurídica en torno al fenómeno de Internet", en *Cuadernos de Derecho Judicial*, CGPJ, Madrid, 2000; Citado por: Antonio Abellán Albertos, cit. p. 10.

4.1. El bien jurídico protegido

En general, el bien jurídico protegido en los apartados del art. 197 del CP es, como se conoce, mayoritariamente, la intimidad personal o familiar.[92] No obstante, aunque parece haber consenso en relación al bien jurídico protegido, concretamente, por el apartado segundo del artículo 197 CP, el mismo ha sido objeto de debate.

A pesar de que parezca que el bien jurídico protegido en este tipo penal es la intimidad, al igual que en el apartado 1 del mencionado precepto, si se analizan los delitos recogidos en este segundo apartado, se concluye que "las conductas afectan a datos que no están en la esfera de custodia del titular, sino en bancos de datos y pueden causar perjuicios a terceros distintos del propio sujeto al que se refiere la información concernida." (STS 379/2018 de 23 de julio).[93]

Es por ello que, tal y como aclara CADENA SERRANO[94] mediante el análisis de la STS 412/2020, de 20 de diciembre, "un sector doctrinal considera que en el art. 197.2 se protegen, en realidad, dos bienes jurídicos. Por una parte, la intimidad del sujeto pasivo, en relación con las conductas de apoderarse, acceder y utilizar los datos. Y, por otra parte, la integridad de los datos, en relación con los comportamientos de modificar o alterar. Distinción, no obstante, relativa por el hecho de quien pretende modificar o alterar, primero debe acceder, con lo que se habría lesionado también la intimidad en estas modalidades de conducta."

De manera que se entiende que "(...) mientras el artículo 197.1 CP, en el primer apartado, custodia la estricta intimidad relacionada con los papeles, cartas o mensajes de correo electrónico o con otros documentos o efectos personales, el artículo 197.2 CP (...) mira más al habeas data informática, esto es, la libertad informática entendida como derecho del ciudadano a controlar la información personal y familiar que se encuentra recogida en ficheros de datos, lo que constituye una dimensión positiva de la intimidad (...). Por tanto, el artículo 197.1 y el artículo 197.2 CP representan diversas modalidades de protección del derecho a la intimidad, con especial contemplación del desarrollo de los sistemas informáticos (...)" (STS. 412/2020, de 20 de julio).

---

[92] Mª Ángeles Rueda Martín, cit. p.34.
[93] Antonio Zárate Conde, cit. p. 2.
[94] Fidel Ángel Cadena Serrano, "La autodeterminación informativa y el derecho penal", pp. 10-11, *Diario La Ley*, nº 9754, (2020). Url: https://laleydigital-autodeterminación-informativa

No solo los tribunales se han pronunciado en ese sentido en numerosas ocasiones, sino que, además, varios autores se han referido a ello. Así por ejemplo, señala MORALES PRATS que lo que protege el art. 197.2 del CP es "la libertad informática frente a un elenco de conductas que implican abusos informáticos contra la misma."[95] Por su parte, MARTÍN-CASALLO LÓPEZ considera que las conductas tipificadas en el art. 197.2 del CP hacen referencia a atentados contra la intimidad personal cometidas sobre datos que se encuentran registrados en soportes informáticos, electrónicos o telemáticos, entendiendo que la protección penal de las denominadas "libertades informáticas" deriva de un derecho de control del titular sobre sus datos personales.[96]

En definitiva, como aclara la STS 586/2016, de 4 de julio, "el bien jurídico objeto de protección no es la intimidad, entendida en el sentido que proclama el artículo 18.1 de la Constitución Española, sino la autodeterminación informativa a que se refiere el artículo 18.4 del texto constitucional. (...)".

De manera que, y teniendo en cuenta que el titular de los datos tiene derecho a exigir que determinados datos personales no sean conocidos, queda reconocido un derecho a la autodeterminación informativa; una libertad informativa, entendida como la libertad de decidir qué datos personales pueden ser obtenidos y tratados por otros. En otras palabras, y como señala la doctrina, la llamada libertad informática es el derecho a controlar el uso de los mismos datos introducidos en un programa informático y comprende, entre otros aspectos, "la capacidad del ciudadano para oponerse a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención" (STC 94/1998 de 4 de mayo, STC 292/2000 de 30 de noviembre, STC 173/2011 de 7 de noviembre, STS 586/2016 de 4 de julio y STS 379/2018 de 23 de julio).[97]

[95] Morales Prats, "El Código Penal de 1995 y la protección de datos personales", *Jornadas sobre el Derecho español de la Protección De Datos,* Agencia de Protección De Datos; Citado por: Antonio Abellán Albertos, cit. p. 2.
[96] Martin-Casallo López, cit.; Citado por: Antonio Abellán Albertos, cit. p. 2.
[97] Antonio Zárate Conde, cit. p. 3.

4.2. La conducta típica

En todo tipo hay una conducta, entendida como comportamiento humano, que constituye el núcleo del tipo, es decir, su elemento más importante.[98] En cuanto a la conducta típica regulada en el precepto objeto de estudio, encontramos el apoderamiento de datos, la utilización de los mismos, su modificación y alteración y el acceso por cualquier medio a los datos.

Si bien es cierto que en ambos incisos del art. 197.2 CP el objeto de la acción delictiva es el mismo y que la acción es prácticamente la misma, se observa una diferencia en cuanto a la intensidad de la acción.[99]

En sus dos incisos, este precepto sanciona primero al que "se apodere, utilice o modifique en perjuicio de tercero" y posteriormente al que "sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero" (art.197.2 CP).

Por lo tanto, en el primero se tipifican las acciones de apoderamiento, utilización o modificación de datos reservados de carácter personal o familiar de otro, que se hallen registrados de forma electrónica en ficheros o en cualquier otro tipo de archivo o registro público o privado; siendo necesario para su consumación que dichas acciones se lleven a cabo sin autorización y en perjuicio de tercero. Y en el segundo inciso el acceso por cualquier medio a los datos personales o familiares de otro y su alteración o utilización en perjuicio del titular o de un tercero.

En relación a las acciones nucleares previstas en este apartado segundo, la STS 412/2020 de 20 Jul. 2020, ECLI: ES:TS:2020:2736, ha establecido qué debe entenderse por las mismas, señalando lo siguiente:

- *"apoderarse*: la traslación de los datos (impresión, transmisión, fotocopiado...) a otro soporte para su posesión;
- *utilizar*: hacer uso de los datos, emplearlos o aprovecharse de los mismos; lo que no comporta necesariamente su aprehensión física;

[98] Francisco Muñoz Conde. Derecho Penal. Parte General. Editorial: Tirant lo blanch. 10º edición, revisada y puesta al día con la colaboración de Pastora García Álvarez, p. 244. Capítulo XV "Tipicidad."

[99] Francisco Soto Nieto, cit. p. 1.

- *modificar*: transformar o cambiar los datos;
- *acceder*: entrar o tener acceso a los datos, por quien ab initio no está autorizado;
- *alterar*: dañar o estropear los datos; y
- *utilizar* (con el mismo sentido en ambos incisos).”

4.3. El objeto

Todas estas conductas típicas recaen sobre datos reservados de carácter personal o familiar automatizados registrados en ficheros o soportes informáticos, electrónicos o telemáticos o en cualquier otro tipo de archivo público o privado, siendo este el objeto de protección. Por tanto, para que los hechos puedan encajar en el art. 197.2 CP “debe exigirse que se trate de un conjunto organizado de información relativa a una generalidad de personas; o que tiene por objeto datos reservados que pertenecen al titular pero que no se encuentran en su ámbito de protección directo, directamente custodiados por el titular, sino inmersos en bases de datos, en archivos cuya custodia aparece especialmente protegida (...) (SSTS 1328/2009, 1084/2010, 40/2016, 168/2016, 634/2019).”

Conforme dispone el artículo 4.1 RGPD ha de entenderse por "datos personales" toda información sobre una persona física identificada o identificable. Los datos de carácter reservado son aquellos que no son susceptibles de ser conocidos por cualquiera. (STS 392/2020 de 15 de julio de 2020).

De acuerdo con lo establecido en este precepto, los datos deben estar registrados en “ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado”. En este sentido, se entiende por fichero “todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica” (art. 4.16) RGPD).

Se trata de ficheros o registros de acceso y uso limitado a personas concretas y con finalidades específicas que recogen datos reservados que pertenecen al titular no custodiados directamente por el mismo, sino que se encuentran inmersos en bases de datos cuya protección se refuerza mediante la autorización necesaria para acceder a las mismas. Estos ficheros o soportes informáticos recogen tanto datos personales propios

como datos de terceros, por lo que la actuación puede ser en perjuicio del titular de los datos o de un tercero.[100]

4.4. El sujeto activo y pasivo[101]

El primer elemento objetivo del injusto que ha de tenerse en cuenta es el sujeto activo, aquella persona que comete el delito, la acción típica.

El sujeto pasivo del delito, en este caso, es el titular de los datos personales o familiares a los que se refiere el precepto. El perjudicado puede ser el sujeto pasivo, o puede ser un tercero.

Por su parte, el sujeto activo del delito regulado en el apartado segundo del artículo 197 CP puede ser cualquier persona, no siendo necesaria ninguna condición personal especial para su autoría, así lo cree JORGE BARREIRO[102], salvo que el autor sea, a su vez, la persona encargada o responsable de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o la autoridad o funcionario público, resultando aplicable, respectivamente, el tipo agravado del art. 197.4 CP y el delito del artículo 198 del CP.

En este sentido, el apartado 4 del artículo 197 específica la pena impuesta por la comisión de estos delitos en función de quién sea el sujeto activo, siendo mayor cuando sea cometido por una persona encargada o responsable de los ficheros, o si los hechos se realizan utilizando de forma no autorizada los datos personales de la víctima.

Por su parte, el subtipo agravado del artículo 198 del Código Penal resulta aplicable cuando quien realiza las conductas antes mencionadas es una autoridad o un funcionario público en el desempeño de su labor profesional, sin mediar causa legal por delito, y prevaliéndose de su cargo. Esto es, cuando quien comete el delito es personal de la sanidad pública.[103]

---

[100] Antonio Zárate Conde, cit. pp. 3-7.
[101] Antonio Zárate Conde, cit. pp. 7-8.
[102] Jorge Barreiro, A., Capítulo I: Del descubrimiento y revelación de secretos. Artículo 197, en el colectivo "Comentarios del Código Penal. Tomo VII.", dirigido por Cobo Del Rosal, p. 128.
[103] En esta línea, señala la STS 616/2022, de 22 de junio, que "no es suficiente con la condición de funcionario público del sujeto activo. (...) El artículo 198 del Código Penal exige algo más: que la actuación del sujeto no esté amparada por la Ley, que el acceso ilícito a la intimidad se

Atendiendo al supuesto objeto de estudio de este trabajo de fin de grado, el sujeto activo es el profesional sanitario que sin estar autorizado, sin consentimiento y sin relación asistencial que lo justifique, accede a la historia clínica electrónica de un tercero. En este sentido, la STS 1328/2009 recuerda que el propio precepto aclara que el delito lo comete el que accede, se apodera, modifica, altera o utiliza los datos "sin estar autorizado" para ello, sin ser datos al alcance de cualquiera. Así lo hace saber también MARTÍN-CASALLO LÓPEZ, al señalar que las conductas contempladas en el art. 197.2 CP requieren que se lleven a cabo por el sujeto activo sin autorización alguna para ello.[104]

Por otro lado, cabe destacar que los problemas en la sistemática del artículo 197 no se encuentran únicamente en la distinción entre las conductas reguladas en el apartado primero y segundo, sino que surgen también problemas interpretativos en la configuración de este último apartado, el cual está estructurado en dos incisos.[105]

Para interpretar la diferencia entre ambos incisos se han defendido varios criterios. En primer lugar, algunos autores consideran que la diferencia se encuentra en el objeto de la conducta, otros autores señalan que la diferencia se encuentra en el sujeto al que se produce el perjuicio típico exigido, y otros defienden que la misma está en la posición subjetiva del autor. A pesar de que el Tribunal Supremo, en un principio, considerase que el criterio para distinguir ambos incisos residía en la diferencia en la intensidad de la acción entre las conductas de apoderamiento y acceso a los datos reservados[106], la doctrina centra su diferencia en "la posición subjetiva del autor en relación con los datos" (STS 412/2020 de 20 de julio). En este sentido, es necesario diferenciar aquella situación en la que se esté o no autorizado para acceder a ellos.[107]

---

produzca en una situación en la que no medie una causa o investigación por delito, y que el sujeto actúe con prevalimiento de cargo (…) que actúe en el área de sus funciones específicas, de tal modo que (...) si su actuación no se refiere específicamente a tales funciones y únicamente se ha aprovechado de su condición (...), su actuación deberá ser calificada conforme al artículo 197 del Código Penal."

[104] Martin-Casallo López, cit. p. 40. Citado por: Antonio Abellán Albertos, cit. p. 10.

[105] Carlos Trincado Castán, "Análisis jurisprudencial de los delitos contra datos reservados desde la perspectiva de la ciberseguridad", en *Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial*, vol. II: Ciberseguridad y ciberdelitos, dir. por Carlos María Romeo Casabona y edit. por Mª Ángeles Rueda Martín (Granada: Editorial Comares, 2023), pp. 209-240.

[106] Carlos Trincado Castán, cit. pp. 209-240.

[107] Julián García Marcos, "El perjuicio como elemento nuclear del artículo 197.2 del Código Penal", p. 2, *Diario La Ley*, nº 10227 (2023). Url: https://laleydigital-perjucio-elemento-nuclear

En cuanto a las conductas descritas, y sobre todo, al acceso no permitido a la información reservada, cabe destacar que la autodeterminación informativa del titular de los datos resulta vulnerada tanto si es una persona ajena a la base de datos o fichero la que accede a los datos protegidos en ficheros tutelados por el propio titular de los datos o por terceros (extraneus), como una persona autorizada fuera del ámbito de dicha autorización bajo cuya tutela se encuentra el fichero o registro quien se apodera, los altera o modifica (intranei). Varias son las sentencias que se remiten a esta idea señalando que "el acusado podía estar autorizado para acceder a la información (...), pero solamente en el desempeño de su función y desde luego nunca para hacer un apoderamiento ilícito." (STS 1328/2009, de 30 de diciembre, STS 377/2013 de 3 de mayo y STS 532/2015 de 23 de septiembre).

Por lo tanto, en caso del intraneus, se trata de una persona que, si bien está inicialmente autorizada, se extralimita en esta autorización, pudiendo darse dos motivos. Ya sea porque estando autorizado "para acceder a los datos y para realizar con ellos las operaciones previstas por el responsable del fichero de acuerdo con la ley, no lo está para otras conductas", o porque se trata de "personas que realizan consultas a las bases de datos de las que obtienen información mediante el empleo de su clave personal que permitía entrar a las mismas, si bien por la asignación de funciones, no le correspondieran tareas en esa específica área, en ese nivel, o en relación a esos concretos datos consultados" (STS 412/2020, de 20 de julio).

Como la principal diferencia entre los extraneus e intraneus es la posibilidad de acceso a los ficheros informáticos, en el caso de los intraneus y teniendo en cuenta que el acceso puede ya estar autorizado, ha de considerarse la conducta de apoderamiento en un sentido amplio, entendiéndose como un desplazamiento posesorio. Por el contrario, para los extraneus, se hace referencia al acceso, siendo este una conducta previa al apoderamiento. De manera que, en relación al extraneus al registro, una vez realizado el acceso ilícito son irrelevantes el resto de comportamientos previstos consistentes en 'alterar' o 'utilizar', ya que quedan absorbidos por el previo acceso, excepto que sea necesaria una prueba relativa a los otros comportamientos para establecer el perjuicio que menciona el tipo.

En definitiva, nos encontramos ante el primer inciso del art.197.2 CP cuando el sujeto activo, que estando autorizado para operar en los ficheros, pero excediéndose en

sus facultades concedidas, se apodere, utilice o modifique los datos en ellos registrados y el segundo inciso se da cuando el sujeto activo es un ajeno a dicho sistema que accede a los datos registrados en ellos o se apodere de ellos o los utilice.

A pesar de que la postura adoptada en la STS 412/2020, de 20 de julio, parecía solucionar esta cuestión, lo cierto es que se han seguido enjuiciando conductas realizadas por sujetos inicialmente autorizados utilizando elementos típicos del segundo inciso. Por lo que, se trata de una cuestión no del todo consolidada, teniendo que analizar las interpretaciones y argumentos de futuras sentencias.[108]

En relación con los accesos a datos reservados contenidos en soportes informáticos por extranei, existen muy pocos pronunciamientos del Tribunal Supremo, y menos en relación a accesos por parte del personal sanitario.

4.5. Elementos subjetivos del injusto: alcance y concepto del "perjuicio"

Habiendo analizado en el anterior epígrafe los elementos objetivos del tipo del injusto del artículo 197.2 CP, se procede ahora a estudiar en este apartado el elemento subjetivo del injusto, el cual resulta más complicado de probar.

En el primer inciso de este artículo, el tipo subjetivo está constituido por el dolo, esto es, la conciencia y voluntad de realizar un apoderamiento, utilización o modificación de datos en perjuicio de terceros. Por su parte, en el segundo inciso, el dolo se refiere a la conciencia y la voluntad de realizar un acceso y utilización o alteración en perjuicio al titular de los datos o de un tercero.[109]

Respecto al perjuicio y la consumación del tipo delictivo, surgen varias cuestiones que resulta interesante aclarar. En esta línea, conviene clarificar cuál es el alcance del perjuicio y de los datos de carácter personal en relación a dicho perjuicio, así como cuándo se consuma el mismo, si con el simple acceso a la base de datos o siendo necesaria la producción del perjuicio para su consumación. En este sentido, se plantea la duda de si el perjuicio es considerado un elemento subjetivo del injusto o no, existiendo un debate

[108] Carlos Trincado Castán, cit. pp. 209-240.
[109] Mª Ángeles Rueda Martín, cit. p. 122.

doctrinal al respecto. Algunos autores entienden la expresión empleada en el primer inciso "en perjuicio de tercero", y la empleada en el inciso final "en perjuicio del titular de los datos o de un tercero" como un elemento subjetivo del injusto y otros no. La mayor parte de los supuestos analizados no consideran el perjuicio como un elemento subjetivo del injusto.

Por un lado, un sector doctrinal entiende la expresión "en perjuicio de tercero" como un elemento subjetivo del injusto, considerando, por tanto, que el propósito de perjudicar a otro debe predominar sobre la conducta de apoderamiento, utilización o modificación de los datos, sin que sea necesaria la efectiva producción de resultado alguno para su consumación.

No obstante, esta postura no es compartida por un mayor sector doctrinal que considera que esta expresión no debe ser interpretada como un elemento subjetivo del injusto, sino que debe ser interpretado como el resultado de la conducta, lo cual implica que como consecuencia del apoderamiento, utilización o modificación se haya causado un perjuicio (STS 803/2017, de 11 de diciembre y STS 234/1999, de 17 de junio).

Así, por ejemplo, de acuerdo con RUIZ MARCO "La referencia textual al perjuicio, en las modalidades que lo contienen, debe ser interpretada como el resultado propio de la acción, resultado que se produce siempre que un tercero accede a los datos que el ciudadano medio mantiene reservados para sí mismo o para su entorno más próximo."[110] De hecho, y conforme a la STS 1391/2000, de 14 de septiembre de 2000, con cita de la STS 234/1999, de 18 de febrero de 1999, el delito objeto de estudio se consuma cuando el sujeto activo accede a los datos.

Como se observa, la interpretación del art.197.2 del CP genera dudas en cuanto al concepto y alcance del "perjuicio" y el concepto de datos reservados de carácter personal o familiar abarcados por la protección penal para la consumación del delito. En este sentido, es preciso saber qué sentido se ha de dar a la expresión "en perjuicio de", así como concretar cuáles son los datos reservados a los que la norma se refiere.

Para resolver estas cuestiones, y llegar a una conclusión firme, se toma de referencia la mencionada STS 234/1999, de 18 de febrero, que, siguiendo con esta línea, señala que "parece razonable que no todos los datos reservados de carácter personal o

[110] Francisco Soto Nieto, cit. pp. 3-4.

familiar puedan ser objeto del delito contra la libertad informática. Precisamente porque el delito se consuma tan pronto el sujeto activo "accede a los datos (…) es por lo que debe entenderse que la norma requiere la existencia de un perjuicio añadido para que la violación de la reserva integre el tipo, un perjuicio que (...) puede afectar al titular de los datos o a un tercero", señala, además, que este perjuicio se "produce siempre que se trata de un dato que el hombre medio de nuestra cultura considera "sensible" por ser inherente al ámbito de su intimidad más estricta (…)" (STS 234/1999 de 18 de febrero, 1328/2009 de 30 de diciembre, STS 532/2015 de 23 de septiembre, STS 40/2016 de 3 de febrero, STS 803/2017 de 11 de diciembre y STS 379/2018 de 23 de julio).

De acuerdo con la STS 234/1999, de 18 de febrero, MARTIN CASALLO extrae las siguientes conclusiones[111]:

- El delito se consuma en cuanto el sujeto activo accede a los datos, por lo que, es necesario un perjuicio añadido, afectando así al titular de los datos o a un tercero.

- Existe una presunción iuris tantum de que las conductas cometidas contra datos sensibles siempre ocasionarán el perjuicio requerido y, por tanto, en esos casos resulta de aplicación el tipo penal. De hecho, respecto a ello, la STS 532/2015, de 23 de septiembre añade que "la conducta sería atípica si no se acreditara el perjuicio para el titular de los datos o que éste fuera ínsito, por la naturaleza de los datos descubiertos, como es el caso de los datos sensibles."

Asimismo, en el tipo que analizamos, y conforme a la analizada sentencia, "el perjuicio producido por la acción tiene que estar abarcado por el dolo pero no tiene que ser el único o principal móvil de la acción." Por lo tanto, según la doctrina mayoritaria y la Jurisprudencia del TS, el delito recogido en el art. 197.2 CP es un delito doloso, pero no de tendencia, ya que el delito se consuma cuando se accede a los datos.[112] De hecho, JAREÑO y DOVAL entienden el perjuicio como un elemento objetivo, ya que no añade nada a la conducta específica de acceso, la cual se efectúa con su mera consideración

[111] Antonio Abellán Albertos, cit. p. 10.
[112] Marcos Ayjón, Miguel, "Las múltiples implicaciones de la protección de datos en la justicia penal", *La ley penal: revista de derecho penal, procesal y penitenciario*, nº 132 (2018), p.13. Url: https://laleydigital-justicia-penal

objetiva, entendiendo, por tanto, este elemento como resultado lesivo abarcado por el dolo.[113]

Teniendo esto en cuenta, surge otra cuestión a analizar. Si se restringe mucho el ámbito de la intimidad protegida, el perjuicio se asimila al "núcleo duro de la privacidad" (salud, ideología, vida sexual, creencias, etc.) el cual ya queda contemplado como subtipo agravado en el art. 197.5, suponiendo la inaplicación del art. 197.2 CP. Sobre esta cuestión se incidirá más adelante junto al análisis de la jurisprudencia, concretamente junto al estudio de la STS 178/2021 de 1 de marzo de 2021.

Por otro lado, el segundo inciso del art 197.2 está redactado de la siguiente manera: "iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.", incluyendo, tal y como aclara la STS 123/2009 de 3 de febrero, tres figuras que son: el apoderamiento, utilización o modificación de datos, el mero acceso, y la alteración o utilización.

Como se puede observar de la redacción del precepto, este perjuicio, en principio, sólo es exigido respecto del apoderamiento, utilización o modificación en el primer inciso y, concretamente, de la alteración o utilización en el segundo; no exigiendo tal perjuicio de tercero para el caso del acceso a los datos personales. Es por ello que se plantea la cuestión de si cabe hablar del perjuicio, del titular de los datos o de un tercero, sólo en relación con el apoderamiento o utilización o también sobre el acceso.

En este sentido, para que no cupiera duda alguna, la redacción debería quedar de forma similar a como sigue: "iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los datos, los altere o utilice en perjuicio del titular de los mismos o de un tercero." De acuerdo con lo indicado en la STS 412/2020, de 20 de Julio de 2020, la principal diferencia se encuentra en la intensidad de la acción entre el apoderamiento y el acceso.

A este respecto, el Tribunal Supremo cree que "es necesario realizar una interpretación integradora en el sentido de que como en el inciso primero, se castigan idénticos comportamientos objetivos que el segundo inciso (apodere, utilice, modifique)

[113] Jareño y Doval, "Revelación de datos personales, intimidad e informática", *El nuevo Derecho Español.Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz,* Aranzadi, 2001, págs. 1486-90. Citado por: Antonio Abellán Albertos, cit. p. 11.

no tendría sentido de que en el mero acceso no se exija perjuicio alguno y en conductas que precisan ese previo acceso añadiendo otros comportamientos, se exija ese perjuicio, cuando tales conductas ya serían punibles -y con la misma pena- en el inciso segundo." (STS 123/2009 de 3 de febrero).

En este sentido, aconseja que también sea exigible (STS 3092/2018 de 28 de junio). De hecho, en su Sentencia 312/2019 de 17 de junio, cierra este debate concluyendo que "pese a que desde una interpretación gramatical pudiera entenderse que la exigencia de perjuicio no cubre a la modalidad típica del acceso (…) sí es exigible el perjuicio desde una interpretación integradora del tipo penal, pues no tendría sentido que se exigiera el perjuicio para los comportamientos delictivos consistentes en apoderarse, utilizar y modificar, y no se exigiera para el acceso, cuando las anteriores conductas típicas requieren el acceso para su realización."[114]

Por lo tanto, el tipo penal objeto de estudio requiere de un perjuicio de tercero al castigar a aquel que sin estar autorizado "se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro", así como a quien "acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero" (art. 197.2 CP).

Con el fin de despejar cualquier duda acerca de estas cuestiones se analizarán algunos supuestos jurisprudenciales recientes, y en el ámbito sanitario, en los que se hayan enjuiciado hechos constitutivos de un posible delito de descubrimiento y revelación de secretos del artículo 197.2 del Código Penal.

5. Análisis jurisprudencial

Este apartado tiene por objeto ejemplificar, a través de un análisis jurisprudencial, todo lo expuesto hasta ahora. En él se pretende hacer hincapié en el concepto del "perjuicio" y las consecuencias jurídico-penales del acceso a historiales clínicos de pacientes por parte de profesionales sanitarios.

Se expondrán algunos supuestos en los que el sujeto activo haya sido condenado por un delito de descubrimiento y revelación de secretos del artículo 197.2 del Código

[114] Julián García Marcos, cit. p. 2.

Penal, teniendo, asimismo, lugar la aplicación del artículo 198 CP ya que, por regla general, los supuestos enjuiciados guardan relación con personal sanitario de la Administración Pública. Además, se manifestarán, mediante el estudio de condenas absolutorias, las razones por las cuales no se considera consumado el delito enjuiciado.

5.1. Supuestos de condena como autor responsable del delito de descubrimiento y revelación de secretos del art. 197.2 CP

En primer lugar, se exponen detalladamente tres supuestos en los que se analiza el acceso ilícito a los historiales médicos de terceros por parte de enfermeras, resaltando lo que la jurisprudencia concluye en relación al acceso a datos de carácter personal y el perjuicio con el fin de conocer cuándo queda consumado el tipo del art. 197.2 CP.

En los tres supuestos a analizar se revuelve el recurso de casación interpuesto por las profesionales sanitarias que alegan una indebida aplicación del artículo 197.2 del Código Penal en relación con el artículo 198 del mismo texto legal y que se infringe tanto la Ley de Protección de Datos (actualmente la LOPDyGDD) como la LAP. En todos ellos, es la Sala Segunda, de lo Penal, del Tribunal Supremo la que confirma la condena de varias enfermeras del Servicio Público de Salud por un delito contra la intimidad, que valiéndose de su profesión, conociendo la regulación contenida en el artículo 7 LAP sobre el carácter confidencial de los datos referentes a la salud de la persona, que no estaban autorizadas para el acceso y que su conducta no estaba justificada, accedieron al historial clínico de pacientes no asignados[115].

- **Supuesto 1**

Siguiendo en esta línea, resulta interesante analizar, en primer lugar, la STS 178/2021, de 1 de marzo, ECLI: ES:TS:2021:743[116], por la que se condena a una enfermera del Servicio Público Aragonés de Salud por un delito contra la intimidad.

[115] "Conforme a la normativa que reconoce y regula el derecho a la intimidad en el marco sanitario, el acceso a un historial clínico de un paciente está permitido siempre que se trate de un paciente "asignado" al profesional que va a efectuar la consulta. Fuera de estos casos, esto es, cuando se trata de un paciente no asignado, el acceso habrá de ser por motivo justificado (...)" (STS 250/2021 de 17 Mar. 2021 (AH.2).

[116] Carlos Peñalosa Torné y Lucía Matarredona Chornet, cit. pp. 2-4.

El 30 marzo 2017 la enfermera mantuvo una conversación con una antigua amiga con la que ya no tenía relación, en la cual dijo que "(...) sabía que su hermana tenía el VIH, (...) y otras palabras en el sentido de que iba desvelar información médica a la que tenía acceso por su profesión". Tras estas declaraciones, la perjudicada denunció los hechos con el fin de que se detectasen los accesos realizados por la acusada a su historial clínico, quedando acreditado tal acceso hasta en dos ocasiones; en diciembre de 2016 y en enero de 2017.

La Audiencia de instancia condenó a la acusada como autora de un delito continuado de descubrimiento de secretos, previsto en los artículos 197.2 y 198 del Código Penal. Ante ello, se interpuso recurso de apelación por la defensa de la acusada, y éste fue desestimado.

Frente a ello, la acusada presentó recurso de casación por indebida aplicación de dichos artículos, alegando el previo conocimiento del historial médico de la perjudicada y de su familia, que accedió a los mismos por mera curiosidad, y afirmando no haber lugar a perjuicio al no concurrir un menoscabo para el bien jurídico tutelado por la norma penal, considerando, por tanto, que la conducta no es típica. Asimismo, la denunciante presentó recurso de casación por indebida inaplicación del párrafo 5 del artículo 197 CP.

- **Supuesto 2**

Por otro lado, y en este mismo sentido, resulta también de interés mencionar la STS 250/2021, de 17 de marzo, ECLI: ES:TS:2021:1090, que estima el recurso de casación contra la SAP de Valladolid y condena a una enfermera, que prestaba sus servicios como funcionaria sanitaria en Valladolid, y que accedió en febrero de 2016 al historial clínico de un paciente no asignado, así como al de sus hijos, sin causa justificada y por simple curiosidad, sin llegar a difundir ni comunicar a nadie los datos a los que tuvo acceso. La paciente, también profesional sanitaria, se dio cuenta de dichos accesos al consultar en el historial clínico de su hijo una medicación y denunció los hechos.

La Audiencia de instancia absolvió a la acusada del delito de descubrimiento y revelación de secretos que, teniendo en cuenta la doctrina más reciente (STS de 28 de Junio de 2018), que aclara que dada la gravedad de las penas asociadas al tipo de revelación de secretos, es necesaria una grave afectación de la autodeterminación informativa, es decir, del bien jurídico protegido, así como determinar en cada caso el

grado de afectación al mismo con el fin de decidir si la conducta merece o no reproche penal, consideró que la conducta no merecía reproche penal y redujo los hechos al ámbito disciplinario.

Frente a ello, y tras interponer recurso de apelación ante el Tribunal Superior de Justicia de Castilla y León (que falló en el mismo sentido), se interpuso recurso de casación.

- **Supuesto 3**

Por último, cabe mencionar la reciente STSJ de Castilla y León nº 343/2023, 27 de enero de 2023, que confirma la SAP de León nº 289/2022, de 16 de mayo, por la que se condena a una enfermera que accedió hasta en 18 ocasiones a las historias clínicas de su compañera de trabajo.

- **Fundamentación jurídica**

Una vez expuestos los hechos acontecidos en los supuestos destacados, se procede a analizar los argumentos aportados por el Tribunal Supremo en relación al objeto del delito, el alcance del perjuicio y la concurrencia del apartado 5 del artículo 197 CP para fallar en dicho sentido.

En estos supuestos, nos centraremos en la conducta a que se refiere este caso, el acceso inconsentido a datos personales alojados en bases de datos. Conforme a este Tribunal, "ese acceso permite una información sobre datos reservados. (…) Por tanto, ha de estarse a lo que refleja el hecho probado, se accedió a la información reservada que fue obtenida a través del acceso no autorizado y la recurrente accedió, de forma inconsentida y no justificada, a la base de datos de salud. (…) Consecuentemente, concurren en el hecho probado los elementos del tipo penal del art. 197 del Código Penal" (STS 178/2021, de 1 de marzo).

En relación al recurso interpuesto por el que se dicta la STS 178/2021, de 1 de marzo, el Tribunal aclara que la acusada no aporta ninguna prueba sobre el previo conocimiento de los datos. Conforme al Tribunal Supremo, la falta de autorización y consentimiento de su titular es el elemento común a todas estas conductas típicas descritas en el art.197.2 CP y que "La exigencia del perjuicio, es común a todas las conductas, y así resulta de la expresión típica y, de otra parte, no tendría sentido su exigencia en

conductas que suponen una mayor intensidad en el ataque y no en el mero acceso." (STS 178/2021, de 1 de marzo).

Además, y en esta misma línea, afirma la STS 250/2021, de 17 de marzo, que la acción es constitutiva del delito tipificado en el artículo 197.2 CP ya que se trata de un acceso al programa informático que recoge la información personal de los pacientes del servicio público de salud. Asimismo, señala que no es necesario haber difundido los datos posteriormente para que se consuma el tipo penal.

Respecto la concurrencia del perjuicio al titular del dato, precisa ser destacado que aunque el art. 197.2 CP emplea la expresión "en perjuicio de", la jurisprudencia no ha considerado el perjuicio como un elemento subjetivo del injusto; entendiendo este perjuicio como un elemento objetivo del tipo necesario para la tipicidad del hecho. No obstante, se apreciará perjuicio en función de la naturaleza del dato al que se accede (STS 250/2021, de 17 de marzo). De hecho, "(...) En la jurisprudencia de esta Sala se han estudiado situaciones semejantes a las que se describen en el hecho probado, destacando el carácter reservado de algunas bases de datos que son gestionadas por la administración pública, como es el caso de la sanidad, (...) Respecto a las que gestionan datos sobre la salud, hemos considerado que, además de reservados, contienen datos sensibles que integren por sí mismos el perjuicio típico, (...) En Sentencias como 497/2018 de 23 octubre, 42/18, de 10 enero, y otras, hemos contemplado los supuestos de los historiales médicos alojados en bases de datos de organización sanitaria." (STS 178/2021, de 1 de marzo).

Por lo tanto, teniendo en cuenta que "los ficheros, que gestionan datos sobre la salud, además de reservados, contienen datos sensibles, (...)" y como "los datos referentes a la salud integran el núcleo duro de la privacidad", se "rellena las exigencias del perjuicio típico que se refiere el artículo 197.2 del Código Penal objeto de la condena", apareciendo ínsito el perjuicio típico en la conducta de acceso (STS 374/2020, de 8 julio).

De hecho, ya en la Sentencia 1328/2009, el 30 diciembre, del Tribunal Supremo se indicó que "estos datos sensibles son, por sí mismo, capaces de producir el perjuicio típico que exige el artículo 197 del Código Penal, (..) y comporta ese daño a su derecho a mantener los secretos ocultos (intimidad) integrando el perjuicio exigido por la norma. En los datos no sensibles sería preciso acreditar la concurrencia del perjuicio."

En este sentido, cuando se trata de alguno de los datos sensibles recogidos en el apartado 5 del artículo 197 CP, el perjuicio consiste en el simple conocimiento del dato a consecuencia del mero acceso, sin que sea necesario un perjuicio añadido pues la propia naturaleza del dato descubierto ya genera un perjuicio. Por el contrario, cuando se trata de un dato no calificado como sensible, debe quedar acreditada la efectiva concurrencia de un perjuicio para que se consuma el tipo delictivo del artículo 197.2 CP (STS 43/2022 de 20 de enero).

Por otro lado, se procede ahora a analizar la cuestión mencionada en el apartado "4.5. Elementos subjetivos del injusto: alcance y concepto del perjuicio" relativa a la concurrencia del apartado segundo y quinto del artículo 197 del Código Penal cuando nos encontramos ante datos reservados que quedan dentro del "núcleo duro de la privacidad" (salud, ideología, vida sexual, creencias, etc.) el cual ya queda contemplado como subtipo agravado; cuestión que también se menciona en la STS 250/2021 de 17 de marzo, la cual se remite a la STS 178/2021, de 1 de marzo, por la que se resuelve el recurso de casación interpuesto en el primer supuesto.

Respecto a ello, como ya se ha mencionado, en el primer supuesto expuesto, la paciente presentó recurso de casación por inaplicación del párrafo 5 del artículo 197 del Código Penal, en virtud del cual, "cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior". La recurrente alega que tratándose de datos de carácter personal afectantes a la salud, la pena aplicable es la prevista en el apartado 5 del art. 197 Código Penal.

Ni el tribunal de primera instancia ni el de apelación aplican este precepto pues consideran que dicha aplicación supondría una vulneración de la interdicción del bis in ídem. De manera que se estaría teniendo en cuenta dos veces la afectación de datos sensibles, una para que dé lugar a la tipicidad del art. 197.2, y otra para la agravación del apartado 5.

En este sentido, resulta de interés aclarar la diferencia entre ambos apartados, que se encuentra en la naturaleza de los datos a los que se accede.

Tal y como aclara el Tribunal en la citada sentencia, los datos a los que hace referencia el 197.2 Código Penal, son datos reservados personales o familiares -incluidos los relativos a la salud- que se hallen registrados en ficheros o soportes informáticos, mientras que los del apartado 5 del art. 197 Código Penal, aunque también son datos reservados de carácter personal, tienen la peculiaridad de que revisten una especial gravedad por revelar la ideología, religión, creencias, salud, origen racial o vida sexual, o respecto de personas necesitadas de especial protección, o cuando la víctima sea menor de edad.

Aclara el tribunal que es necesario "interpretar la concurrencia de ambas posibilidades" con el fin de evitar una "doble valoración de la salud, -como elemento que rellena el perjuicio típico del art. 197.2 del Código Penal y como elemento de agravación del apartado 5 del art. 197 del Código Penal-."; siendo estos últimos supuestos especialmente graves que han de ser interpretados como tipo agravado cuando se manifiesta una especial intensidad en la afectación de los datos relativos a la salud, cuando en el hecho concurran unas consideraciones específicas por las que resultan afectadas la dignidad de la persona, su honor, o un perjuicio relevante distinto de la salud, que sea consecuencia del acceso injustificado e inconsentido, cuando concurra una especial lesividad o dañosidad en función del dato descubierto o cuando tenga lugar la afectación y concurrencia del daño junto a otros bienes jurídicos. Por lo tanto, la aplicación del tipo agravado requiere de un mayor desvalor.

Concretamente, en el primer supuesto en el que se alega la falta de aplicación de este subtipo agravado, el tribunal no considera que en el hecho probado concurra esa especial gravedad. Además, de acuerdo con el tribunal, no se planteó en el juicio "la trascendencia e importancia del dato reservado, que no por ello pierde la naturaleza de dato sensible, pero como tipo agravado respecto de otro básico menos gravoso, requiere que además de su contenido sensible resulte una especial afectación del bien jurídico, o la afectación a la dignidad del sujeto pasivo, o su concurrencia con otros bienes afectados; extremos que ni se declaran probados ni han sido objeto de debate y valoración por el tribunal del enjuiciamiento." Es por ello que, en ese supuesto concreto, se desestima el recurso interpuesto por la paciente en relación a la inaplicación del apartado 5 del art.197 CP.

5.2. Supuestos de absolución del delito de descubrimiento y revelación de secretos del art. 197.2 CP

Por otro lado, resulta interesante, en primer lugar, destacar algunos supuestos por los que profesionales sanitarios, que aprovechando su condición, sin que existiera razón asistencial alguna y sin autorización, hayan sido absueltos como autores responsables del delito de descubrimiento y revelación de secretos tras acceder al historial clínico de pacientes; así como conocer las razones jurídicas aportadas por los tribunales para fallar en ese sentido.

- **Supuesto 1**

En primer lugar, es preciso destacar la STS 392/2020, del 15 de julio de 2020, ECLI: ES:TS:2020:2509,[117] por la que se absuelve a un médico de servicio público de salud, que en 2011, se limitó a consultar en un par de ocasiones la historia clínica electrónica de un paciente con el fin de conocer si constaban bajas laborales por incapacidad temporal.

Fue condenado por la Audiencia Provincial de A Coruña en aplicación del artículo 197.2 CP en relación con el artículo 198 del mismo texto legal, tras afirmar que "la comprobación de la existencia de un parte de baja por incapacidad temporal laboral supone acceder a datos sobre la salud, se desconoce qué datos concretos pudo examinar y constatar, que el acceso debe entenderse a datos especialmente sensibles sujetos a la especial protección del artículo 197.6 (actual 197.5) del Código Penal y que el perjuicio causado se ha producido con el mero conocimiento de esos datos especialmente sensibles."

No obstante, el condenado considera que los hechos son atípicos por no haberse producido perjuicio, el cual ni siquiera fue acreditado por la acusación, y por no haber accedido a datos reservados o sensibles. Por ello, el doctor recurrió en casación.

[117] Eduardo De Urbano Castrillo, "Si se accede a datos no sensibles y que son de conocimiento público, no hay delito contra la intimidad", pp. 1-3, *Diario La ley*, obtenido del libro "Derecho penal económico: 61 defensas de éxito", edición nº 1 (2022). Url: https://laleydigita-accesodatosnosensibles

- **Supuesto 2**

Asimismo, conviene resaltar la Sentencia del Tribunal Superior de Justicia de Asturias 43/2021 de 16 de octubre, ECLI: ES:TSJAS:2021:2460, por la que se resuelve el recurso de apelación interpuesto por una profesional sanitaria del Servicio de Salud del Principado de Asturias, contra la sentencia dictada por la Audiencia Provincial de Asturias.

La acusada accedió en varias ocasiones a los datos de otro médico de profesión, y de quien se encontraba divorciada, para obtener información acerca de su salud. En 2019, tres días antes del acceso, el titular de los datos envió un correo electrónico a su hija en el que le comentaba la posibilidad de padecer una enfermedad y el tratamiento médico a recibir.

La Audiencia Provincial de Asturias condenó a la médico como autora responsable de un delito de descubrimiento y revelación de secretos. Frente a ello, interpuso recurso de apelación invocando, entre otros motivos, la vulneración del art. 197 del Código Penal, al considerar que no existía un perjuicio para terceros.

- **Supuesto 3**

En el mismo sentido, cabe destacar la STS 312/2019, de 17 de junio, ECLI: ES:TS:2019:2028, mediante la que se resuelve el recurso de casación interpuesto por la acusadora particular contra la sentencia dictada por la Audiencia Provincial de Guadalajara, por la que se confirma la absolución como autor responsable de un delito de descubrimiento y revelación de secretos a su ex marido, que fue su médico de cabecera hasta diciembre de 2010, situación que cambió tras la ruptura matrimonial debido a unas lesiones que él le provocó y por las que fue denunciado.

En 2011 consultó el parte de asistencia de su exmujer del que tenía previo conocimiento pues éste constaba en la denuncia que ella interpuso contra él. En 2013, con el fin de preparar el juicio oral, realizó un acceso a una radiografía que el propio acusado, como su médico de cabecera, le había prescrito en 2010. Además, no queda acreditado que gracias a dichos accesos el acusado tuviera conocimiento de datos nuevos relativos a su salud.

De modo que la Audiencia absolvió al profesional sanitario. Frente a ello, ella interpuso recurso de casación por indebida inaplicación del art 197.2 y 198 del Código Penal.

- **Supuesto 4**

Por último, se expone la STS 1328/2009, de 30 de diciembre de 2009, ECLI: ES:TS:2009:8457, que resuelve el recurso de casación interpuesto por un profesional sanitario que había sido condenado por acceder a la historia clínica de un paciente obteniendo el nombre de su médico de cabecera.

- **Fundamentación jurídica**

El Tribunal Supremo considera que "desde una visión amplia, todo dato que se extrae de una "historia clínica" tiene relación con la salud de la persona a la que pertenece, pero en el ámbito penal debemos, además, considerar si la conducta enjuiciada ha producido un menoscabo sustancial en el bien jurídico tutelado por el tipo recogido en el artículo 197.2 del Código Penal (...)" (STS 7/2020, de 23 de abril de 2020).

En este sentido, recuerda algunos precedentes de condena más destacados, como por ejemplo, la STS 586/2016, de 4 de julio, por la que "se condenó, en aplicación del artículo 197.2 del Código Penal a un médico del Servicio Público de Salud que, se aprovechó de su cargo para acceder en numerosas ocasiones a bases de datos de historiales médicos, sin autorización ni justificación", así como la STS 532/2015, 23 de septiembre, por la que se condena a un profesional sanitario del Insalud que, una vez más, aprovechándose de su condición, consultó el historial clínico de varios compañeros sin su consentimiento.

No obstante, de acuerdo con el Tribunal, tales supuestos, en relación a la lesión del bien jurídico protegido por el artículo 197.2 del Código Penal, se alejan bastante de los hechos que ahora se presentan.

De hecho, el tribunal recuerda la STS de 17 de junio de 2019, que realiza un estudio de la jurisprudencia para diferenciar los supuestos de condena de las absoluciones tomando como criterio diferenciador "una fundada y grave afectación del bien jurídico protegido". En este sentido, "las condenas siempre constataron en el caso enjuiciado "una intrínseca gravedad" de los supuestos a los que se enfrentaban. Mientras que las

absoluciones entendían que "no había menoscabo sustancial del bien jurídico tutelado" (...)"

Por lo tanto, "el perjuicio para un tercero, en este caso para el titular del derecho a la intimidad vulnerado por el acceso a sus datos clínicos personales, es un elemento ineludible para poder considerar que se ha producido un hecho típico y punible." (STSJ de Asturias 43/2021 de 16 de octubre).

Como se ha explicado, mediante cita jurisprudencial, si se produce un acceso a datos relativos a la salud nos encontramos ante datos sensibles que por su propia naturaleza ocasionan un perjuicio a terceros. No obstante, si no se trata de datos sensibles, ha de analizarse si dicho acceso ocasiona o no tal perjuicio.

Por ello, resulta necesario analizar, en el primer supuesto, si dicho acceso a la pestaña de altas y bajas del programa informático produjo algún perjuicio. Para llegar a una conclusión, el tribunal se remite a las ya explicadas STS 803/2017, de 11 de diciembre y STS 234/1999, de 18 de febrero. De hecho, recuerda que la propia sentencia recurrida (Sentencia 111/2018, de 8 de octubre de 2018 de la Audiencia Provincial de A Coruña) afirma que, conforme al informe emitido por la Inspección Sanitaria, las bajas médicas no están registradas en el programa de acceso a la historia clínico-laboral a través del cual accedió el doctor, que el conocimiento de dichas bajas los tuvo por otros medios, que no se sabe qué datos pudo consultar y que no queda probado que entrara en otra pestaña del historial médico que no fuera aquella que recoge las altas y bajas médicas. Por lo tanto, el Tribunal Supremo confirma que no consta que algún dato relativo a la salud haya sido transmitido a terceros, precisamente por la imposibilidad de haber tenido conocimiento de alguno de ellos debido al tiempo de acceso y la pestaña a la que se accedió donde no había ningún apunte respecto a la existencia de bajas laborales. Por lo tanto, no pudo haber obtenido ningún dato personal del denunciante, sino más bien todo lo contrario, la inexistencia de bajas.

Teniendo en cuenta todo lo expresado, el Tribunal Supremo estima el recurso, rechaza el carácter sensible de la información obtenida y concluye no haberse generado perjuicio.

Respecto al segundo supuesto, la Sala del TSJ de Asturias entiende que fue el mensaje que recibió la hija del denunciante lo que empujó a su exmujer a realizar la

consulta de la historia clínica. Además, se desconocía que se hubiera realizado un tratamiento distinto más allá del acceso a estos datos, lo que impide afirmar que concurra el requisito del perjuicio de tercero, por no quedar acreditado en este caso. Consecuentemente, la profesional sanitaria es absuelta del delito por el que había sido condenada.

Con el fin de resolver el recurso interpuesto en el supuesto 3, la Sala reproduce la jurisprudencia de esta Sala al señalar que "Se trata de un delito que supone el conocimiento y voluntad en la acción realizada actuando a sabiendas, en tanto que el perjuicio se refiere al peligro de que los datos albergados en las bases de datos protegidas puedan llegar a ser conocidos por personas no autorizadas. (...) El perjuicio se realiza cuando se apodera, utiliza, modifica o accede a un dato protegido con la intención de que su contenido salga del ámbito de privacidad en el que se incluyó en una base de datos, archivo, etc, especialmente protegido, porque no es custodiado por su titular sino por titulares de las bases con especiales exigencias de conductas de protección." (STS 40/2016, de 3 de febrero).

Por lo tanto, reiterando lo señalado en numerosas ocasiones, declara que no consta acreditado tal perjuicio ni tampoco que el acusado actuara con ánimo de causárselo, pues el acusado ya conocía su historia clínica por otro medio legítimo, sin que hubiese tenido acceso a datos nuevos relativos a la salud de su exmujer. De modo que la sala desestima el recurso de casación y confirma íntegramente la sentencia dictada por la Audiencia, absolviéndolo del delito por el que se le acusa.

Por último, respecto al cuarto supuesto, el Tribunal Supremo, en la STS 1328/2009, de 30 de diciembre de 2009, señala que "el único dato que el acusado obtuvo con uso inadecuado del programa informático de consulta clínica, fue el relativo al nombre del médico de cabecera". El Tribunal Supremo, y teniendo en cuenta que la historia clínica recoge el contenido mínimo de la misma en el art.15.2 LAP, aclara que "en los dieciséis datos que enumera (el art.15.2 de la mencionada ley) no se refiere al nombre del facultativo, dato, por tanto, que aunque pudiera referirse a la intimidad personal, no puede entenderse secreto o reservado de los efectos del tipo del art. 197.2 CP, (...)"

De hecho, tal y como recalca el tribunal, "la propia Administración Sanitaria considera que no se debe proteger como dato accesible y privado el nombre del médico

de cabecera, siendo un dato totalmente inocuo dentro del historial clínico del paciente, no pudiendo equipararse el acceso al conocimiento de un dato médico como puede ser el conocimiento de una enfermedad con el acceso a un dato meramente administrativo."

En definitiva, como "el dato del médico de cabecera no es un dato que el hombre medio de nuestra cultura considera "sensible" (...) pues es un dato de conocimiento público, al menos potencial -y no inherente a la intimidad, dato administrativo al alcance de todos los empleados del Centro- (...)" (SSTC. 73/82, 57/94), el condenado fue absuelto del delito de descubrimiento y revelación de secretos del artículo 197.2 del Código Penal.

5.3. Balance ante el análisis jurisprudencial del delito de descubrimiento y revelación de secretos del art. 197.2 CP

En definitiva, podemos concluir que la línea jurisprudencial mayoritaria y en relación con los datos sensibles contenidos en la historia clínica, a diferencia de lo que sucede con el resto de datos, y teniendo en cuenta que los datos relativos a la salud afectan a la esfera o núcleo duro de la intimidad y son especialmente sensibles y relevantes, el mero acceso a los mismos conlleva un perjuicio; colmando así las exigencias del tipo, sin necesidad de un ánimo adicional.

Además, en el supuesto de que se vincule con alguna de las situaciones recogidas en el apartado 5, habrá de aplicarse el tipo agravado. En este sentido, si es de aplicación el tipo básico por haber descubierto datos sensibles relacionados con la salud, y en consecuencia, haber ocasionado un perjuicio, no será aplicable el tipo agravado salvo que concurra alguna de las circunstancias mencionadas.

Por lo tanto, para poder encajar la acción en el tipo básico se ha de producir un perjuicio; perjuicio que se genera siempre que el objeto del delito sean datos relativos a la salud, de lo contrario, tal perjuicio debe ser probado.

En este sentido, y basándose en la doctrina del Tribunal Supremo, se aprecia en los tres primeros supuestos de condena "la concurrencia de los elementos del delito señalado y previsto en el artículo 197.2 in fine del código penal, pues la(s) acusada(s) accede(n) sin autorización y sin motivo asistencial alguno a datos reservados y considerados sensibles, como los que atañen a la salud de la persona, que forman parte de

la más estricta intimidad, produciéndose de este modo el perjuicio (...)" (STSJ de Castilla y León nº 343/2023).

Como se observa, aunque, en general, el acceso a la historia de un paciente es constitutiva de delito, cuando no existe perjuicio por no tratarse de datos sensibles o por conocer previamente la información no resulta típica la conducta.

6. Conclusiones

Primera.-

La historia clínica recoge aquellos documentos que guardan datos de carácter personal, relacionados mayoritariamente con la salud, y que son, por naturaleza, particularmente sensibles. De hecho, resulta imprescindible el archivo de la historia clínica, siendo esta una obligación legalmente recogida en la Ley 41/2002, de 14 de noviembre.

Segunda.-

El sistema de almacenaje y preservación de la Historia Clínica, y consecuentemente, la atención sanitaria, se ha visto mejorado con la llegada de la digitalización. En este sentido, la digitalización de la historia clínica, en cuanto que permite el conocimiento rápido, centralizado y actualizado de los datos en ella contenida, ha facilitado una asistencia sanitaria de mayor calidad y accesibilidad tanto para los profesionales sanitarios como para los propios pacientes.

Tercera.-

A pesar de las ventajas que la digitalización otorga, la historia clínica electrónica extraña riesgos ya que facilita la comisión de delitos de descubrimiento y revelación de secretos en cuanto que resulta más accesible. Estos delitos, regulados entre los artículos 197 y 201 del Código Penal, protegen el derecho a la intimidad y la autodeterminación informativa, siendo este el bien jurídico protegido.

Cuarta.-

La legitimidad de acceso a la historia clínica por parte de los profesionales sanitarios que intervienen en el proceso asistencial queda motivada, precisamente, por la

finalidad asistencial. El acceso a la historia clínica, regulado por normas deontológicas y jurídicas, debe quedar justificado por una relación asistencial entre profesional sanitario y paciente, ya sea de forma directa o indirecta por colaboración en el proceso asistencial.

Quinta.-

Se ha de estar autorizado para el acceso a la historia clínica pues, de lo contrario, si se ocasiona un perjuicio al titular de los datos o a un tercero, el acceso a la Historia Clínica sin mediar justificación alguna para el tratamiento del paciente siempre constituirá delito.

La Historia Clínica, y consecuentemente, todos aquellos datos personales en ella contenidos, quedan protegidos por la obligación de secreto profesional regulada en el art.199.2 CP y la protección de ficheros regulada en el art.197.2 CP.

El deber de secreto profesional existe debido a la relación asistencial entre profesional sanitario y paciente, impidiéndole al sanitario la divulgación de la información confidencial conocida. La prohibición del acceso al historial clínico médico de los pacientes no asignados no deriva de la obligación de guardar secreto profesional sino de la de la obligación de respeto hacia los datos de otro registrados en los ficheros, existiendo un "deber de autodeterminación informativa".

Sexta.-

Un asunto especialmente controvertido es la interpretación del art. 197.2 CP. Por lo que resulta necesario aclarar cómo se solucionan los supuestos de acceso a la Historia Clínica. En este sentido, las conductas cometidas contra datos sensibles, por su propia naturaleza, siempre ocasionan el perjuicio requerido, resultando de aplicación el artículo 197.2 del Código Penal. De hecho, no todo acceso a dato de carácter personal o familiar produce un perjuicio. Es por ello que, como el delito se consuma en cuanto el sujeto activo accede a los datos, es necesario un perjuicio añadido. De modo que si no se trata de un dato sensible es necesario acreditar dicho perjuicio pues de lo contrario la conducta sería atípica.

Tras analizar varios supuestos resueltos por los tribunales, se puede concluir que cuando el acceso se realiza a datos sensibles existe perjuicio y se condena a los profesionales sanitarios como autores del delito de revelación de secretos del artículo 197.2 del Código penal en aplicación con el artículo 198 del Código Penal cuando los

sanitarios lo sean de la Administración Sanitaria Pública. No obstante, si bien es cierto que la historia clínica contiene, en su mayoría, datos sensibles, recoge también información relativa a la salud pero no de carácter sensible. Es en este último caso cuando no se genera perjuicio a terceros, salvo que el mismo quede acreditado.

Séptima.-

La redacción del actual art. 197.2 CP resulta compleja y confusa, incluso para la doctrina que ha calificado su redacción como "diabólica, atormentada e inacabable". Tal es la confusión que no queda claro si debe exigirse el perjuicio para el acceso ya que este perjuicio, en principio, sólo es exigido respecto del apoderamiento, utilización o modificación en el primer inciso y de la alteración o utilización en el segundo. No obstante, a pesar de que parezca que no se exige tal perjuicio de tercero para el acceso a los datos personales, los tribunales consideran que este precepto debe interpretarse de forma que se entienda exigible el perjuicio también para el acceso.

Para que no cupiera duda alguna, y que no se generase inseguridad jurídica, sería conveniente revisar este delito que, a la vista de la realidad de la digitalización, puede cobrar cada vez más relevancia. De hecho, cada vez más casos de accesos ilícitos terminan en manos de los tribunales; así lo hace constar la reiterada y actual jurisprudencia de los tribunales, habiendo sido el Tribunal Supremo quien haya aunado todas aquellas cuestiones que generaban una división doctrinal y jurisprudencial.

7. Referencias bibliográficas

Abellán Albertos, Antonio. "Protección penal de los datos de carácter personal y de los programas informáticos". *Diario La Ley*, nº 5811 (2003): 1750-1769. Url: https://laleydigital-protecciónpenaldatos

Aberasturi Gorriño, Unai. "Los principios de la protección de datos aplicados en la sanidad". Tesis doctoral. Servicio Editorial de la Universidad del País Vasco, 2011. Url: https://addi.ehu.es/ABERASTURI.pdf

Antomás, J. y Huarte del Barrio, S. "Confidencialidad e historia clínica. Consideraciones ético-legales". An. Sist. Sanit. Navar, Vol. 34, nº 1 (2011). Url: https://scielo.isciii.es/pdf/asisna/v34n1/revision2.pdf

Aulló Chaves, Manuel y Pelayo Pardos, Santiago. "La historia clínica." En De Lorenzo y Montero, R. (Coordinador General) *Plan de formación en responsabilidad legal profesional.* Unidad didáctica número 1. Madrid: Edicomplet. Asociación Española de Derecho Sanitario, 1997.

Baños Jiménez, Juan Pedro et al. *Manual de la Relación Médico-Paciente.* España: Foro de la Profesión Médica de España, 2019. Url: https://manual-relacion-medico-paciente.pdf

Beltrán Aguirre, Juan Luis, García López, Fernando José y Navarro Sánchez, Carmen. *Protección de Datos Personales y Secreto Profesional en el ámbito de la Salud: Una propuesta normativa de adaptación al RGPD.* Barcelona: Sociedad Española de Salud Pública y Administración Sanitaria, 2017. Url: https://SESPAS_proteccion_datos_2017.pdf

Cadena Serrano, Fidel Ángel. "La autodeterminación informativa y el derecho penal". *Diario La Ley*, nº 9754 (2020). Url: https://laleydigital-autodeterminación-informativa

Casanova Asencio, Andrea Salud. *Protección de datos en el ámbito de la historia clínica el acceso indebido por el personal sanitario y sus consecuencias.* Barcelona: Indret, 2019. https://indret.com/2019/07/1463.pdf

De Miguel Sánchez, Noelia. "Secreto Médico, Confidencialidad e Información Sanitaria". *Marcial Pons*, Madrid, 2003.

De Urbano Castrillo, Eduardo. “Si se accede a datos no sensibles y que son de conocimiento público, no hay delito contra la intimidad”. *Diario La Ley*, obtenido del libro "Derecho penal económico: 61 defensas de éxito", edición nº 1 (2022). Url: https://laleydigita-accesodatosnosensibles

Emaldi Cirión, Aitziber. “El ciberespacio como nuevo escenario para vulnerar derechos fundamentales”. En *Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial,* vol. II: Ciberseguridad y ciberdelitos, dirigido por Carlos María Romeo Casabona y editado por Mª Ángeles Rueda Martín, pp. 101-125. Granada: Editorial Comares, 2023.

Ferrer Gelabert, Sandra.“E-salud: La tecnología al servicio de la salud”. En *E- salud, autonomía y datos clínicos: Un nuevo paradigma,* dirigido y coordinado por Cristina Gil Membrado, pp. 13-31. Madrid: Dykinson, 2021.

García Garriga, Jesús. “El acceso indebido a los datos clínicos por personal sanitario y la aplicación de los art. 197 y 198 del CP: aproximación a dos recientes sentencias de hechos idénticos y fallos dispares”. *Juristas de la salud*, Vol. 25, nº 2 (2015). Url: https://www.accesoindebido-2020-05/vol25n2_07_Estudio.pdf

García Marcos, Julián. “El perjuicio como elemento nuclear del artículo 197.2 del Código Penal”. *Diario La Ley*, nº 10227 (2023). Url: https://laleydigital-perjucio-elemento-nuclear

García Ortega, Cesáreo y Cózar Murillo, Victoria. “La intimidad del paciente: novedades legislativas”. *Medicina Clínica* 115 (2000): 426-427, DOI:10.1016/S0025-7753(00)71579-X

Gracieta Royo, Luis Pedro e Ibarra García, Nuria. “La confidencialidad de la historia clínica: una aportación desde la perspectiva del contrato de seguro.” *Diario La Ley* (2000). Url: https://laleydigital-confidencialidad

González Rodríguez, Raidel y Cardentey García, Juan. “La historia clínica médica como documento médico legal”. *Revista Médica Electrónica.* (2015), ISSN 1684-1824. Url: http://scielo.sld.cu/scielo.hc_documento_médico_legal

Herrán Ortiz, Ana Isabel. “Datos personales de salud, investigación científica y tecnología big data. De la necesidad de un marco normativo propio en la UE”. En *E-*

salud, autonomía y datos clínicos: Un nuevo paradigma, dirigido y coordinado por Cristina Gil Membrado, pp. 179-216. Madrid: Dykinson, 2021.

Jareño y Doval. "Revelación de datos personales, intimidad e informática". *El nuevo Derecho Español. Estudios Penales en Memoria del Profesor José Manuel Valle Muñiz.* Aranzadi, 2001.

Jareño Leal, Ángeles. "El secreto profesional del médico. Referencia especial a los pacientes menores de edad". *La ley penal: revista de derecho penal, procesal y penitenciario,* nº 32, (2006). Url: https://laleydigital-secreto-profesional

Jorge Barreiro, A.. Capítulo I: "Del descubrimiento y revelación de secretos. Artículo 197". En *"Comentarios del Código Penal. Tomo VII"*, dirigido por Cobo Del Rosal.

Jove Villares, Daniel. "La protección de datos: un derecho para el entorno digital", Juventud y constitución: un estudio de la Constitución española por los jóvenes en su cuarenta aniversario, coord. por Andrés Iván Dueñas Castrillo, Daniel Fernández Cañueto, Gabriel Moreno González, 2018, ISBN 9788494620140, págs. 79-102. Url: https://actas14_juventud_constitucion_dig.pdf

Jove Villares, Daniel. *La protección de lo sensible, o cuando la naturaleza del dato no lo es todo.* Valencia: Tirant lo blanch, 2023.

Júdez, Javier, Nicolás, Pilar, Delgado, M. Teresa, Hernando, Pablo, Zarco, José y Granollers, Silvia. "La confidencialidad en la práctica clínica: historia clínica y gestión de la información". *Medicina Clínica* 118 (2002):18–37, DOI:10.1016/S0025-7753(02)72271-9

Lucas Murillo de la Cueva, Pablo. "El derecho fundamental a la protección de los datos relativos a la salud". En *Estudios de protección de datos de carácter personal en el ámbito de la salud*, editado por Santiago Ripol Carulla y coordinado por Jordi Bacaria Martrus, pp. 21-43. Barcelona: Marcial Pons, 2006.

Marcos Ayjón, Miguel. "Las múltiples implicaciones de la protección de datos en la justicia penal". *La ley penal: revista de derecho penal, procesal y penitenciario*, nº 132 (2018). Url: https://laleydigital-justicia-penal

Martín-Casallo López, Juan José. “Problemática jurídica en torno al fenómeno de Internet”, en *Cuadernos de Derecho Judicial,* CGPJ, Madrid, 2000.

Mayordomo Rodrigo, Virginia. “Un supuesto de colisión de deberes: la obligación de denunciar y el mantenimiento del secreto profesional”. *Actualidad Penal,* nº 33 (2002). Url: https://laleydigital-colisión-deberes

Méjica García, Juan. “El Enfermo Transparente. Futuro Jurídico de la Historia Clínica Electrónica”. *Edisofer*, Madrid, 2002.

Morales Prats, Fermín. “El Código Penal de 1995 y la protección de datos personales”. *Jornadas sobre el Derecho español de la Protección De Datos,* Agencia de Protección De Datos, 1997.

Muñoz Conde, Francisco. “Tipicidad”. En *Derecho Penal. Parte General.* Revisada y puesta al día con la colaboración de Pastora García Álvarez, 235-247. Valencia: Tirant lo blanch, 2019.

Muñoz Marín, Ángel. “Descubrimiento y revelación de secretos de historial clínico”. *Revista Ceflegal. Cef,* núm. 153 (2013): 188-192. Url: https://revistas.cef.udima.es/ceflegal/article

Nicolás Jiménez, Pilar. “El concepto de dato médico y genético”. En *Estudios de protección de datos de carácter personal en el ámbito de la salud*, editado por Santiago Ripol Carulla y coordinado por Jordi Bacaria Martrus, pp. 77-101. Barcelona: Marcial Pons, 2006.

Nicolás Jiménez, Pilar. “La protección jurídica de los datos genéticos de carácter personal”. Tesis Doctoral, Universidad de Deusto, 2006.

Nolla, Joan Miquel.“La importancia de la Historia Clínica”. En *El dolor en las enfermedades reumáticas,* España: Editorial Aresta SC, 2008.

Otero González, Pilar. “Delitos contra la intimidad, derecho a la propia imagen e inviolabilidad del domicilio”. En *Memento Práctico Francis Lefebvre. Penal Económico y de la Empresa*, Madrid, 2011.

Peñalosa Torné, Carlos y Matarredona Chornet, Lucía. “El delito de descubrimiento de secretos por el acceso ilícito al historial médico del paciente”. *Diario La Ley*, nº 10366 (2023). Url: https://laleydigital-delito-acceso-ilícito

Portolés, J.M. y Castilla, V. “Desarrollo y utilización de la historia clínica en soporte electrónico: experiencia de un servicio de nefrología de nueva creación.” *Nefrología*, nº 6, (2002): 512-521. Url: https://hc-soporte-electrónico

Prat Westerlindh, Carlos. “Descubrimiento y revelación de secretos por un médico que denuncia irregularidades en implantes mamarios”. *La ley penal: revista de derecho penal, procesal y penitenciario*, nº 107 (2014): 7. ISSN 1697-5758. Url: https://laleydigital-irregularidades-implantes

Ramos-López, J.M, Cuchí Alfaro, M. y Sánchez Molano, M.A. “Archivo de historias clínicas Digitalizado, una solución previa a la Historia Clínica Electrónica”, *Papeles médicos*, vol. 18, Núm. 2 (2009). Url: https://papelesmédico-archivohcdigitalizada

Romeo Casabona, Carlos María. “La protección de datos personales en la Unión Europea. Aspectos sectoriales relacionados con la salud”. En *Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial*, vol. II: Inteligencia artificial y responsabilidad penal, dirigido por Carlos María Romeo Casabona y editado por Mª Ángeles Rueda Martín, pp. 3-26. Granada: Editorial Comares, 2023

Romeo Casabona, “Derecho penal, Parte especial”. En *Comentarios al Código Penal, Vol. II*, p. 255. España: Tirant lo Blanch, 2004. ISBN:9788484560029.

Rueda Martín, Mª Ángeles. *La nueva protección de la vida privada y de los sistemas de informatización en el Código Penal*. Barcelona: Atelier, 2018.

Sacartés Fortuny, Ricard. “Historia clínica electrónica en un departamento de obstetricia, ginecología y reproducción: desarrollo e implementación. Factores clave.” Tesis doctoral, Universitat Autònoma de Barcelona, 2013. Url: https://historiaclínicaelectrónica/tesis/2013.pdf

Salazar Martínez, Laura. “La custodia de las historias clínicas”. *Diario La Ley*, nº 7951, (2012). Url: https://laleydigital-custodia-historia-clínica

Soto Nieto, Francisco. “Revelación de secretos. Entidad del dato revelado”. *Diario La Ley*, nº 6132 (2004). Url: https://laleydigital-laleynext-entidad-dato

Tejero Álvarez, Mercedes. *Documentación clínica y archivo*, 1.ª ed. Madrid: Diaz de Santos, 2003.

Trincado Castán, Carlos. "Análisis jurisprudencial de los delitos contra datos reservados desde la perspectiva de la ciberseguridad". En *Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial*, vol. II: Ciberseguridad y ciberdelitos, dirigido por Carlos María Romeo Casabona y editado por Mª Ángeles Rueda Martín, pp. 209-240. Granada: Editorial Comares, 2023.

Troncoso Reigada, Antonio y González Rivas, Juan José. "Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos personales y Garantía de los Derechos Digitales", Thomson Reuters Aranzadi, 2021, ISBN: 978-84-1346-416-9

Troncoso Reigada, Antonio. "La confidencialidad de la historia clínica". *Cuadernos de Derecho Público*, nº 27, 2006. Url: https://confidencialidad-historia-clínica

Zárate Conde, Antonio. "La tutela penal de los datos de carácter personal. Una perspectiva jurisprudencial". *Diario La Ley*, nº 9422 (2019). Url: https://laleydigital-tutela-penal

Zaldívar Robles, Javier. "La protección penal del derecho a la intimidad". *Teorder* 2016, nº 19, pp. 162-184.