EGUZKILORE
Número 21.
San Sebastián
Diciembre 2007
163 - 183

DELITOS CONTRA LA INTIMIDAD Y NUEVAS TECNOLOGÍAS

Luz María PUENTE ABA
Universidad de A Coruña

Resumen: El desarrollo creciente de las nuevas tecnologías, la informática y destacadamente de Internet ha multiplicado las posibilidades de atentar contra la intimidad personal, principalmente en lo que se refiere a la interceptación de comunicaciones, a la captación y posterior difusión de la imagen, y a la afectación de datos personales recogidos en bases de datos informáticas. El presente trabajo analiza hasta qué punto se compromete la intimidad en cada supuesto concreto, si realmente el Código penal otorga protección frente a tales ataques contra este bien jurídico y, en caso de que no sea así, cuál es el tipo de respuesta que el ordenamiento jurídico puede ofrecer ante estas actuaciones.

Laburpena: Informatika, Internet bereziki eta teknologia berrien garapenak bakoitzaren intimitatearen kontra egiteko aukerak biderkatu ditu, batez ere komunikazio mozketan eta irudiak hartzen eta hedatzen eta informatika datu baseetan hartutako datu pertsonalen erabileran. Lan honek kasu bakoitzak intimitatean duen eragina aztertzen da, Zigor Kodeak ondasun juridikoa babesten baldin badu, eta horrela ez bada, zein den ordenamendu juridikoak eskeintzen duen erantzuna jardun hauen aurrean.

Résumé: Le développement croissant des nouvelles technologies, l'informatique et notamment l'Internet, a multiplié les possibilités d'atteintes contre l'intimité privée, principalement en ce qui concerne l'interception des communications, la captation et diffusion d'images, et l'affectation de données personnelles stockées dans des bases de données informatiques. Le présent travail analyse jusqu'à quel point on compromet l'intimité dans chaque hypothèse concrète, et si le Code pénal accorde une véritable protection face à des attaques contre le bien juridique protégé, et, le cas échéant, quelle est la réponse juridique que la loi peut offrir pour faire face à ces activités.

Summary: The gradual development of new technologies, computer sciences and, especially, Internet increases the possibilities of attempting against the personal privacy, mainly with regard to the communications interception, the reception and diffusion of images, and the use of personal data in computer databases. The present study analyzes the risk to privacy inherent to every particular case and the protection granted to privacy by the Penal code. It also examines the alternative juridical answers that the Law could offer to face those behaviours.

Palabras clave: Derecho penal, derecho a la intimidad, delitos contra la intimidad, nuevas tecnologías.

Gako hitzak: Zigor zuzenbidea, intimitaterako eskubidea, intimitatearen kontrako delituak, teknologia berriak.

(Nota): Contribución a la Jornada sobre "Protección penal de la privacidad en entornos digitales", San Sebastián, 29 noviembre 2007 (subvencionada por el Proyecto DITESEC del programa SAIOTEK, Dpto. de Industria, Comercio y Turismo del Gobierno Vasco).

Mots clef: Droit pénal, Droit à l'intimité, Délits contre l'intimité, Nouvelles technologies.

Key words: Penal Law, Right to privacy, offences against privacy, new technologies.

I. INTRODUCCIÓN

La previsión de los delitos contra la intimidad en nuestro Código penal cuenta ya con una larga tradición; la intimidad de la persona, como bien jurídico de carácter individual, es uno de los intereses que desde siempre ha sido objeto de protección por las normas penales. Así, con carácter general, los artículos 197 y siguientes del Texto punitivo castigan una serie de atentados contra la intimidad personal, y acudiendo a la figura básica de esta categoría delictiva (art. 197.1), se pueden agrupar con carácter genérico en tres bloques fundamentales: el apoderamiento de mensajes, documentos o efectos personales; la interceptación de las comunicaciones; y la utilización de artificios técnicos de captación del sonido o de la imagen.

El desarrollo creciente de las nuevas tecnologías, la informática y destacadamente de Internet ha multiplicado las posibilidades de atentar contra la intimidad personal, principalmente en lo que se refiere a la interceptación de comunicaciones, a la captación y posterior difusión de la imagen, y a la afectación de datos personales recogidos en bases de datos informáticas. De hecho, últimamente los medios de comunicación no dejan de ofrecer noticias relacionadas con la vulneración de la intimidad fundamentalmente en estos tres aspectos: por una parte, la mayor exposición y vulnerabilidad de la intimidad personal inherente a la utilización de Internet, puesto que es sencillo rastrear el uso que un individuo hace de este medio de comunicación; por otra parte, la progresiva extensión y facilidad del empleo de aparatos de filmación de la imagen (cámaras digitales y teléfonos móviles, destacadamente), unido a la posibilidad de que cualquier ciudadano aisladamente pueda difundir luego sin esfuerzo estas filmaciones en Internet ("colgándolas" en páginas web); y por último, la progresiva configuración, tanto por entes públicos como privados, de bases de datos informáticas con datos personales, que por la propia naturaleza de este soporte pueden ser vulnerables frente a intromisiones externas.

El objeto de este trabajo es centrarme en los tres ámbitos mencionados, analizando hasta qué punto se compromete la intimidad en cada supuesto concreto, si realmente el Código penal otorga protección frente a tales ataques contra este bien jurídico y, en caso de que no sea así, se examinará cuál es el tipo de respuesta que el ordenamiento jurídico puede ofrecer ante estas actuaciones.

II. LA PROTECCIÓN DE LOS DATOS PERSONALES CONTENIDOS EN BASES DE DATOS INFORMÁTICAS

Una de las ventajas de la informática es que permite el almacenamiento y tratamiento automatizado de múltiples datos, que así pueden ser adecuadamente ordenados, conservados, modificados y utilizados para los fines que se deseen. Por este motivo, es cada vez más frecuente que tanto las entidades públicas como las privadas alberguen la información que necesiten en bases de datos informáticas, que almacenan una gran cantidad de datos de carácter personal. Las garantías del correcto tratamiento de estas bases de datos se recogen en la Ley orgánica 15/1999, de 13 de diciembre, de protección de los datos personales, que regula los requisitos necesarios para archivar

los datos personales y, destacadamente, para garantizar que su recogida y tratamiento no suponga una vulneración de la intimidad personal.

La pregunta que cabría formularse es si cualquier atentado a los datos personales recogidos en bases de datos informáticas podría constituir un delito contra la intimidad. Obviamente el acceso a bases de datos personales no encajaba en ninguno de los tres grupos tradicionales de conductas delictivas contra la intimidad: apoderamiento de mensajes, documentos o efectos personales; interceptación de comunicaciones; y captación del sonido o la imagen. Por ello el Código penal de 1995, por primera vez, introdujo un tipo penal específico en esta materia, que castiga 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 fichero 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" (art. 197.2 CP).

No obstante, la solución no pasa sin más por crear esta nueva figura típica, sino que realmente hay que comprobar si con tales conductas se está vulnerando el **bien jurídico protegido** en estos preceptos, la intimidad personal. De entrada, puede afirmarse que no resulta fácil el encaje de esta prohibición con el concepto tradicional del bien jurídico "intimidad". Tradicionalmente, la *intimidad* ha venido designando el ámbito puro de privacidad personal del que se excluye a terceros, el espacio vital íntimo de una persona. En este sentido, el Tribunal Constitucional ha otorgado a la intimidad un contenido ciertamente negativo, en el sentido de que este derecho fundamental otorga la facultad de exclusión de los demás de un ámbito cerrado, personal y propio (por ejemplo, STC 231/1988).

Sin embargo, con el paso del tiempo y precisamente en estrecha vinculación con el desarrollo de las nuevas tecnologías, el derecho a la intimidad ha ido adquiriendo también una vertiente positiva, como poder de control sobre la publicidad de la información personal; más aún, con el paso del tiempo llegan a configurarse derecho a la intimidad y derecho a la protección de datos personales como dos derechos autónomos. Con la proliferación de las bases de datos, fomentadas por el desarrollo de la informática, cada vez un mayor número de datos personales pasan a manos ajenas y por lo tanto se vuelven más vulnerables frente a intromisiones no deseadas; por este motivo, se considera que la protección del derecho a la intimidad también debe abarcar el *derecho a controlar los propios datos personales* contenidos en bases automatizadas, de tal modo que el individuo pueda decidir y tener garantizado quién y para qué conoce y utiliza esos datos de carácter personal. Se configura por lo tanto un derecho a disponer de los datos personales en general, que ni siquiera tienen por qué estar referidos a aspectos particularmente íntimos, ni ser datos secretos de acceso restringido, e incluso tampoco tienen por qué estar incluidos necesariamente en bases de datos informáticas: se trata, con carácter general, de garantizar el derecho de controlar la propia información personal como forma de evitar que se produzcan introsimiones ajenas en la intimidad de cada uno (por ejemplo, SSTC 254/1993, 11/1998, 30/1999, 134/1999, 202/1999, 292/2000)[1].

---

1. Vid. sobre la protección que el TC otorga a esta faceta de la intimidad, ROMEO CASABONA, C.M., "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en ROMEO CASABONA, C.M. (coord.), *El cibercrimen: nuevos retos jurídico –penales, nuevas respuestas político–*
…

A la configuración de este bien jurídico responde precisamente la previsión del transcrito artículo 197.2 del Código penal: se castigan determinados atentados contra los datos recogidos en ficheros o bases de datos. Obviamente, los datos son protegidos independientemente del archivo o fichero en el que se encuentren, que no tiene por qué ser informático, tal y como dice expresamente el propio Código penal. Simplemente lo que determinó el castigo de estas conductas es la proliferación de ficheros de datos personales, que se produjo precisamente con el desarrollo de la informática.

Para proteger el bien jurídico tutelado, el derecho de control de la información personal, se sancionan con carácter general las **conductas de apoderamiento, utilización, modificación o acceso a los datos personales** archivados sin tener autorización para ello[2]. A pesar de la casuística empleada por el legislador, éstas son en esencia las actuaciones prohibidas, esto es, formas de intromisión no consentida en los datos ajenos de carácter personal, desde conductas menos lesivas como el mero acceso hasta comportamientos más graves como la modificación de los datos. No resulta difícil encontrar supuestos reales en los que se ha verificado este tipo delictivo: así, por ejemplo, cabe citar la STS 1571/2005, que castiga a un funcionario de Hacienda que, si bien dentro de sus funciones no estaba la de acceder o tratar las bases de datos de la Hacienda pública, consiguió acceder a ellas en su lugar de trabajo y apoderarse de datos allí almacenados.

A efectos de una clarificación de estas conductas delictivas, cabe hacer unas breves precisiones sobre la naturaleza de los datos protegidos y sobre el tipo de ficheros en los que se encuentran archivados.

En relación con los datos objeto de protección, el art. 197 del Código penal menciona expresamente los **"datos reservados de carácter personal o familiar"**. La polémica surge aquí en relación con la referencia a "reservados", puesto que plantea la duda de si se protege cualquier dato archivado en un fichero, o si de entre los datos archivados sólo se van a proteger aquellos que tengan un carácter realmente reservado; esto conduciría, a continuación, a la difícil tarea de otorgar un significado al término "reservado". No hay unanimidad sobre la interpretación de este término, y lo cierto es que posee una indudable relevancia, puesto que si se adopta esta última posición más restringida (protección no de cualquier dato contenido en un fichero, sino sólo de

---

…
criminales, Comares, Granada 2006, pp. 170 y ss; el mismo autor, *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia 2004, pp. 31 y ss; ORTS BERENGUER, E. / ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia 2001, pp. 17 y ss; MATA Y MARTÍN, R.M., "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías", *Revista Penal*, 2006, nº 18, p. 220; HUERTA TOCILDO, S. / ANDRÉS DOMÍNGUEZ, A.C., "Intimidad e informática", *Revista de Derecho penal*, 2002, nº 6, pp. 14 y ss; RUIZ MARCO, F., *Los delitos contra la intimidad*, Colex, Madrid 2001, pp. 45 y ss; GÓMEZ NAVAJAS, J., *La protección de los datos personales*, Aranzadi 2005, pp. 87 y ss.

2. Vid. con carácter general sobre la conducta típica del art. 197.2, GÓMEZ NAVAJAS, *La protección de los datos personales*, pp. 135 y ss; ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, pp. 115 y ss; MORALES PRATS, F., en QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007, pp. 422 y ss; ORTS / ROIG, *Delitos informáticos*, pp. 31 y ss; MORÓN LERMA, E., *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, Aranzadi 2002, pp.60 y ss; RUEDA MARTÍN, M.A., *Protección penal de la intimidad personal e informática*, Atelier, Barcelona 2004, pp. 69 y ss; MATA, "La protección penal de datos", pp. 232 y ss.

los que puedan calificarse como realmente reservados), quedarían desprotegidos los datos "no reservados" frente a estas conductas de acceso, apoderamiento, utilización o modificación.

Partiendo de esta interpretación restrictiva, de entrada ya quedarían fuera del ámbito del art. 197 CP los datos incluidos en ficheros accesibles al público. Según el art. 3 de la Ley de protección de datos personales, son ficheros accesibles al público aquellos cuya consulta puede ser realizada por cualquier persona; según este mismo precepto, tienen la consideración de ficheros de acceso público exclusivamente el censo promocional, los repertorios telefónicos en los términos previstos en su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de pertenencia al grupo; asimismo, tendrán también este carácter los diarios y boletines oficiales y los medios de comunicación. Los datos incluidos en tales ficheros, por ser de acceso público para cualquier persona, ya no podrían tener la calificación de reservados. Partiendo entonces de una equivalencia entre "reservado" y "no público", se integrarían en el ámbito típico sólo los datos de acceso limitado para terceros ajenos al fichero donde se contienen[3]. Esta misma opinión es mantenida, por ejemplo, por la STS 1461/2001, que considera precisamente que el término "reservados" ha de entenderse equivalente a "secretos" o "no públicos".

Por otra parte, aun centrándonos en los ficheros no accesibles al público, si partimos de una interpretación todavía más restrictiva del término "reservados", habría que analizar caso por caso los datos contenidos en cada fichero para determinar cuáles merecen esta calificación y cuáles no, en función de la información que revelan sobre la persona: se trataría entonces de llegar a identificar "reservado" con "íntimo"; efectivamente, partiendo de esta interpretación restrictiva, quedarían excluidos de la protección penal aquellos datos que no puedan considerarse reflejo de la intimidad personal más estricta[4]. Parece que esta posición la defienden algunas resoluciones de nuestros Tribunales; así, cabe citar la SAP Zaragoza 399/2002 (confirmada por la STS 725/2004), que da a entender que la protección penal de los datos reservados abarca únicamente a aquellos que son reflejo de la intimidad más estricta, y la SAP Madrid 118/2005, manifiestando que el tipo del art. 197 CP se refiere a datos que se pretende que no trasciendan de la esfera de la privacidad.

Por consiguiente, lo más adecuado sería partir de la primera interpretación más amplia y entender que todo dato personal incluido en cualquier fichero puede ser objeto del delito del art. 197.2 CP. Por una parte, esta opción resulta más coherente con la definición del bien jurídico aquí protegido: si está siendo tutelada la facultad de disponer de los propios datos personales con carácter general, como vía de garantizar el control sobre la propia información personal, no tiene sentido discriminar entre unos datos y

---

3. Así, entienden que son reservados aquellos datos de conocimiento limitado para terceros ajenos al fichero, ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, pp. 110-111; RUEDA MARTÍN, *Protección penal de la intimidad*, p. 71, citando jurisprudencia al respecto; FERNÁNDEZ TERUELO, J.G., *Cibercrimen. Los delitos cometidos a través de Internet*, CCC 2007, p. 136; MATA, "La protección penal de los datos", p. 229. GÓMEZ NAVAJAS, *La protección de datos personales*, p. 195, considera que los datos protegidos en este precepto son aquellos "no destinados al público conocimiento".

4. Vid. así ORTS / ROIG, *Delitos informáticos*, pp. 32-33.

otros en función de la concreta información que otorguen sobre una persona. Y por otra parte, efectuar una libre valoración sobre qué datos son reservados y cuáles no crea unas altas dosis de inseguridad jurídica, pues queda en la indeterminación qué clase de datos se protegen penalmente. Por lo tanto, lo más adecuado es entender que cabe la protección penal de cualquier dato recogido en un fichero, puesto que todos ellos son datos personales cuyo poder de control ha de quedar precisamente "reservado" para su titular[5]. Esta opinión es puesta de relieve también en alguna resolución judicial; así, la SAP Huelva 76/2006 (confirmada por la STS 358/2007) pone de manifiesto que para muchos autores la expresión "reservados" resulta redundante.

Por último, cabe hacer una breve referencia a la necesidad de que los datos personales han de estar recogidos en **"ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de fichero o registro público o privado"**. Como ya se ha dicho con anterioridad, lo esencial es que los datos se hallen registrados en un fichero, independientemente de su naturaleza. Esto puede llevar a plantearse dos interrogantes: en primer lugar, si cabe incluir en el tipo penal la creación ilegal de los ficheros, la recogida ilegal de datos; y en segundo lugar, si reciben protección los datos incluidos en ficheros de carácter ilegal.

En relación con el primer punto, la respuesta ha de ser obligatoriamente negativa. En el Código penal se castigan conductas que atentan contra los datos personales automatizados, es decir, que ya se encuentran archivados en cualquier tipo de fichero. Obviamente, también atentarían contra la facultad de controlar los propios datos comportamientos como los siguientes: recogida de datos de forma engañosa para crear un fichero, elaboración de ficheros sin seguir todas las formalidades legales, o creación de un fichero para una finalidad distinta de aquellas que constituyen el objeto legítimo de la entidad que lo pretende elaborar. No obstante, este tipo de actuaciones y otras semejantes supondrían en todo caso una vulneración de las previsiones de la Ley de protección de datos personales, de tal modo que en su caso nos encontraríamos ante una infracción administrativa de las previstas en esta Ley orgánica; la intervención penal, por lo tanto, se restringe a las conductas ya mencionadas que atentan contra los datos ya registrados[6].

En segundo lugar, podríamos plantearnos qué ocurre si ya se ha creado ese fichero ilegal, que no respeta los requisitos normativos para su constitución, y posteriormente alguien atenta contra los datos contenidos en ese fichero: ¿se admite la tutela penal de los datos contenidos en ficheros ilegales, o sólo de los registrados con todas las formalidades legales? Lo cierto es que la redacción del art. 197 no aporta una respuesta a

---

5. MORALES PRATS, en QUINTERO OLIVARES, *Comentarios*, pp. 422-423, considera que el empleo de este calificativo no tiene sentido y que "todos los datos personales automatizados quedan protegidos por la conminación punitiva del artículo 197.2 CP". Manifiestan HUERTA TOCILDO / ANDRÉS DOMÍNGUEZ, "Intimidad e informática", p. 59, que el objeto material de este precepto está constituido por "cualquier dato personal registrado". GÓMEZ NAVAJAS, *La protección de los datos personales*, cit., pp. 194-195, tras plantear las diferentes posibilidades de interpretación de este término, y poniendo de manifiesto la dificultad de distinción práctica entre datos reservados y no reservados, propone la eliminación de tal calificativo.

6. Cfr. MORALES PRATS, en QUINTERO OLIVARES, *Comentarios*, p. 422; RUEDA MARTÍN, *Protección penal de la intimidad*, p. 76; MATA, "La protección penal de datos", pp. 230-231; RUIZ MARCO, *Los delitos contra la intimidad*, p. 81.

este interrogante. De entrada, se verificarían aquí infracciones de carácter administrativo, no sólo por la creación ilegal del fichero, sino también por las posibles conductas posteriores de terceros que utilizan ilegítimamente estos datos: la Ley de protección de datos personales castiga con carácter general tratar o usar los datos personales con conculcación de las garantías establecidas en la propia Ley, y es evidente que en estos casos se está tratando de forma ilegal unos datos de carácter personal.

De todas formas, no cabría incluir tal conducta en el art. 197 CP, puesto que no podemos considerar que los datos estén realmente registrados, tal y como exige el tipo penal, si el fichero ha sido creado ilegalmente. Como se ha dicho, las conductas de configuración de ficheros al margen de las exigencias legales constituye una infracción de la Ley de protección de datos personales, y por lo tanto las actuaciones posteriores sobre los datos que contienen estos ficheros constituirá asimismo una infracción de esta naturaleza.

III. LA INTERCEPTACIÓN DE LAS COMUNICACIONES EN RELACIÓN CON EL USO DE INTERNET

De entrada, la aparición de Internet supone el surgimiento de un poderoso medio de comunicación, con múltiples potencialidades; esto también dará lugar, consecuentemente, al aumento de las posibilidades de afectar a la intimidad. En este apartado se analizarán algunas cuestiones básicas relacionadas con el uso de Internet como medio de comunicación: por una parte, se examinará si queda comprendida en el art. 197 la interceptación de las comunicaciones a través de Internet, y por otra parte, se hará referencia a dos situaciones concretas en las que la vulneración de la intimidad en este sentido podría verse justificada.

Como ya se ha puesto de manifiesto, el art. 197 CP castiga **la interceptación de las telecomunicaciones y la captación de cualquier señal de comunicación**. Estas referencias tan genéricas permiten sin problema su aplicación a cualquier conducta que suponga una vulneración del secreto de las comunicaciones, es decir, cualquier intromisión en las comunicaciones ajenas. Por lo tanto, aquí también tendrá cabida la interceptación de las comunicaciones personales a través de Internet, ya sea a través de mensajes de correo electrónico, chats, telefonía por Internet, etc.[7].

Por otra parte, la intimidad de una persona también se puede ver afectada cuando se vigila el uso que hace de Internet como medio de búsqueda de información. De hecho, cada vez existen más modalidades de "spyware", esto es, de programas informáticos que, clandestinamente, recopilan información de los usuarios de Internet sin su consentimiento: qué páginas visitan, qué transacciones comerciales hacen, con quién

7. De hecho, el propio legislador introdujo expresamente la mención de "mensajes de correo electrónico" al lado de las cartas, al sancionar las conductas de apoderamiento al inicio del art. 197. Vid. al respecto ORTS BERENGUER / ROIG TORRES, *Delitos informáticos*, pp. 25 y ss; MORÓN LERMA, *Internet y Derecho penal*, p. 60; FERNÁNDEZ TERUELO, *Cibercrimen*, pp. 123 y ss; RUEDA MARTÍN, *Protección penal de la intimidad*, pp. 41 y ss; ROMEO CASABONA, C.M., "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable", en AAVV, *Estudios jurídicos del Ministerio Fiscal*, II – 2003, pp. 77 y ss; el mismo autor, *Los delitos de descubrimiento y revelación de secretos*, p. 79, 88-91 y 93-95; MATA, "La protección penal de datos", pp. 223 y ss.

se comunican, etc. La realización de tales conductas de "rastreo" encaja asimismo en el tipo penal del art. 197 CP, puesto que supone sin duda una interceptación de señales de comunicación[8].

De hecho, ya es frecuente ver en la jurisprudencia sentencias de condena en relación con estos comportamientos. Así, por ejemplo, la STS 237/2007, que condena a una persona que instaló un programa "spyware" en su ordenador privado para averiguar si lo utilizaba su esposa, y para detectar los chats en los que ella participaba; o también la SAP Málaga 60/2005, que condena a un sujeto por introducir un troyano en un ordenador ajeno para así acceder a su correo electrónico y a todo el contenido de su disco duro.

A pesar del carácter delictivo de estas intromisiones en el uso que una persona hace de Internet, cabe señalar dos supuestos específicos en los que, por diferentes razones, se permite un cierto control o vigilancia de estas actividades. El primer supuesto está referido a las posibilidades de control de los operadores que presten servicios de comunicaciones, y el segundo al control del uso de Internet en el lugar de trabajo.

Para fijar las posibilidades de **control del uso de Internet por parte de los operadores que presten servicios de comunicaciones** hay que acudir a la reciente Ley 25/2007, de 18 de octubre, sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. Esta norma obliga a los operadores que presten servicios de comunicaciones electrónicas o redes públicas de comunicaciones a conservar, durante doce meses, los datos generados en el marco de la prestación de tales servicios, y a cederlos a los agentes facultados, previa autorización judicial, con el fin de detección de delitos graves. Se trata de obligaciones que afectan a las compañías suministradoras de servicios de telefonía fija y móvil y de Internet; los datos que deberán conservar son los relativos a origen y destino de la comunicación, fecha, duración, tipo de comunicación y equipo terminal utilizado. La ley prohíbe terminantemente controlar y conservar el contenido de las comunicaciones electrónicas y la información consultada utilizando una red de comunicaciones electrónicas; esto implica, por lo tanto, que no se puede acceder al contenido de las conversaciones telefónicas ni de otro tipo realizadas a través de Internet, y que tampoco se puede controlar qué información consulta el usuario de Internet. Se trata, simplemente, del deber de los operadores de conservar exclusivamente los datos antes mencionados, con el único fin de cederlos a las autoridades si éstas así lo requieren en el desarrollo de sus actividades de investigación delictiva.

La generalización del uso de ordenadores e Internet en todos los ámbitos de la vida diaria ha determinado también la presencia de estos instrumentos en los lugares de trabajo, y por consiguiente existe el **riesgo de que Internet destacadamente sea utilizado en este ámbito, por parte de los trabajadores, para fines privados o de ocio ajenos a la actividad laboral** (v.gr. enviar correos electrónicos privados, consultar información en Internet).

---

8. Vid. al respecto MORALES PRATS, F., "Internet: riesgos para la intimidad", en AAVV, *Internet y Derecho penal*, CGPJ, Madrid 2001, pp. 72 y ss; MORÓN LERMA, *Internet y Derecho penal*, pp. 31 y ss.

Vid. en general sobre la necesidad de protección penal de las comunicaciones a través de redes telemáticas, ROMEO CASABONA, "La protección penal de la intimidad", pp. 73 y ss.

Esta situación suscita la problemática de cuáles son las facultades de control del empresario sobre el trabajador: por un lado, el empleador tiene derecho a ejercer un cierto control de las actividades realizadas en el lugar de trabajo, con el fin de garantizar el adecuado desarrollo de la actividad laboral; pero por otro lado, estas facultades de vigilancia tienen como límite el respeto de los derechos fundamentales de los trabajadores, como por ejemplo el derecho a la intimidad. Por ello, se plantea cuál es el punto hasta el que llegan estas posibilidades de control del uso que un trabajador hace de Internet, buscando el justo equilibrio entre las facultades de supervisión del empresario y el derecho a la intimidad de los trabajadores. Incluso se podría llegar a plantear si una extralimitación del empleador, vulnerando la intimidad de su subordinado, podría llegar a constituir en algún caso un delito contra la intimidad.

Ciertamente estas situaciones se han planteado con cierta frecuencia en la práctica y han dado lugar a numerosas resoluciones de los Tribunales de lo social. De un examen de la jurisprudencia laboral se puede extraer cuál es, con carácter general, la solución que se suele adoptar en estos casos. Básicamente, se reconoce el derecho de los empresarios a controlar la actividad de los trabajadores, como forma de comprobar que la actividad laboral se está desempeñando adecuadamente. No obstante, no cualquier medida de control es admisible: se podrán adoptar únicamente aquellas medidas que estén justificadas en el caso concreto porque existen sospechas que fundamenten la necesidad de control, y han de ser idóneas y proporcionadas, en el sentido de que no se pueda adoptar para ese fin una medida menos lesiva de los derechos del trabajador (así se ha manifestado el Tribunal Constitucional al respecto: STC 186/2000).

Si examinamos los casos extraídos de la jurisprudencia social, observamos que de todas formas no hay unanimidad en el tratamiento y resolución de estos casos. Existe una línea jurisprudencial que tiende a considerar que el control del uso que un trabajador hace de Internet no supone una vulneración de su derecho a la intimidad, puesto que encaja en las facultades legales de control del empresario, que lleva a cabo esta intromisión con el fin de garantizar el adecuado cumplimiento de las obligaciones laborales. En este sentido, por ejemplo, se manifiestan las STSJ Cataluña 14-11-2000 y 5886/2000[9].

Por otra parte, otra línea jurisprudencial propugna la aplicación de los principios de necesidad y proporcionalidad, admitiendo el control del uso que el trabajador hace de Internet cuando existen razones fundadas para ello y cuando no existen otras medidas de control menos gravosas. Y en todo caso, una cuestión fundamental es que únicamente debe controlarse si el trabajador usa Internet con perjuicio para el desarrollo de la actividad laboral, pero no puede llegar a controlarse el contenido material de esa utilización, es decir, qué paginas web visita, o qué dicen los correos electrónicos que envía. Por ese motivo, en los casos en que el empresario ha llegado a acceder a estos contenidos, los Tribunales de lo social suelen considerar desproporcionada esa medida, puesto que realmente se trata de una invasión de la intimidad del trabajador no justificada por el fin perseguido: para mantener un adecuado control de los trabajadores podrá

9. Vid. al respecto, citando jurisprudencia, FERNÁNDEZ TERUELO, *Cibercrimen*, p. 129.

ser necesario saber si hacen un uso abusivo de Internet, pero nunca será necesario averiguar para qué concretos fines privados lo están utilizando[10].

Clarificadoras al respecto son, por ejemplo, las STSJ Cantabria 48/2007, STSJ Galicia 20-10-2006, STSJ Cataluña 5024/2002; estas sentencias se sitúan en la línea de la STC 186/2000, que estableció que la constitucionalidad de cualquier medida restrictiva del derecho a la intimidad del trabajador viene determinada por la estricta observancia del principio de proporcionalidad, y que ha de configurarse en la medida estrictamente imprescindible para el correcto y adecuado desenvolvimiento de la actividad laboral; se trata de determinar si la concreta medida está justificada, es idónea para la finalidad pretendida, y es asimismo necesaria y equilibrada.

Por último, cabe citar destacadamente la reciente STS 26-9-2007 (Sala de lo Social), que establece dos principios básicos que han de regular el control del uso de Internet por parte del empresario: en primer lugar, "lo que debe hacer la empresa de acuerdo con las exigencias de buena fe es establecer previamente las reglas de uso de esos medios, con aplicación de prohibiciones absolutas o parciales, e informar a los trabajadores de que va existir control y de los medios que han de aplicarse en orden a comprobar la corrección de los usos, así como de las medidas que han de adoptarse en su caso para garantizar la efectiva utilización laboral del medio cuando sea preciso, sin perjuicio de la posible aplicación de otras medidas de carácter preventivo, como la exclusión de determinadas conexiones" (FJ 4º); en segundo lugar, el TS establece que el control empresarial sólo ha de referirse a la averiguación del posible uso personal de Internet, sin llegar a profundizar en conocer el contenido concreto de este uso: "la entrada inicial en el ordenador puede justificarse por la existencia de un virus, pero la actuación empresarial no se detiene en las tareas de detección y reparación, sino que, como dice con acierto la sentencia recurrida, en lugar de limitarse al control y eliminación del virus, «se siguió con el examen del ordenador» para entrar y apoderarse de un archivo cuyo examen o control no puede considerarse que fuera necesario para realizar la reparación interesada" (FJ 5º).

Con carácter general, estos casos llegan a los Tribunales porque el empresario, tras controlar a su trabajador y descubrir el uso que realiza de Internet, lo despide de la empresa; lo que se examina, por lo tanto, es la validez de dicho despido, y en los casos en que la jurisprudencia aplica estos principios y rechaza estas medidas de control por excesivas, suele declarar que tal despido es improcedente. Por consiguiente, esta es la vía por la que generalmente se solucionan estas intromisiones en la intimidad del trabajador, puesto que tales injerencias suelen ser la base de un despido y se acude a los Tribunales de lo social para hallar una solución en el ámbito laboral. Es improbable, por lo tanto, que un Tribunal penal tenga que tratar uno de estos casos, y principalmente porque, según el art. 201 CP, para perseguir los delitos contra la intimidad es necesario denuncia del agraviado; en estos supuestos, la persona afectada suele preferir solucionar esta problemática en el marco del Derecho laboral. En cualquier caso, puede afirmarse que estas conductas de intromisión en la intimidad ajena estarían justificadas

10. Vid. ROMEO CASABONA, "La protección penal de la intimidad", pp. 97-98, y *Los delitos de descubrimiento y revelación de secretos*, pp. 136-137, poniendo de relieve precisamente que el ejercicio legítimo del derecho de control de los trabajadores, por parte del empresario, requiere la proporcionalidad entre la medida de control ejecutada y la afectación del derecho a la intimidad.

por el legítimo ejercicio del derecho de control de los trabajadores, únicamente cuando se respetase la normativa laboral y los principios enunciados por la jurisprudencia social y constitucional; cuando tal injerencia se realice fuera de tales límites, y realmente se verifique una interceptación de comunicaciones o, como expresamente dice el Código penal, un apoderamiento de mensajes de correo electrónico, podría ser posible la integración de esta conducta en el art. 197 CP, al no quedar amparada por el legítimo derecho de control de los trabajadores.

IV. REVELACIÓN DE SECRETOS AJENOS A TRAVÉS DE INTERNET: ESPECIAL REFERENCIA A LA DIFUSIÓN DE IMÁGENES

Como ya sabemos, la figura básica en el marco de los delitos contra la intimidad se refiere a tres grandes bloques de conductas: apoderamiento de mensajes, documentos o efectos personales; interceptación de comunicaciones; y captación del sonido o de la imagen. La realización de estos comportamientos reviste carácter delictivo, según el art. 197.1 CP, siempre que se realicen con intención de vulnerar la intimidad, sin que sea exigible a mayores la difusión de tal información[11]. Cuando se produce la revelación, difusión o cesión de estos datos obtenidos ilícitamente, se estarán realizando las conductas típicas recogidas en el art. 197.3 CP, que contiene dos figuras diferenciadas: en primer lugar, un tipo agravado, que sanciona a quien, después de haber realizado alguna de las conductas del art. 197.1, procede a difundir la información obtenida; en segundo lugar, existe un tipo atenuado, que sanciona a aquel sujeto que, sin haber participado en el descubrimiento ilícito de la información, la obtiene por otras vías (se la comunican, la encuentra por casualidad, etc.) y se limita a difundirla siendo consciente de que ha sido obtenida de forma ilícita.

La realización de estas conductas de difusión de datos atentatorios contra la intimidad cobra una especial significación desde la aparición de Internet. Con este nuevo medio de comunicación, resulta infinitamente más sencillo difundir y hacer pública una determinada información. Existen páginas web en las que cualquier persona sin ningún esfuerzo puede situar contenidos propios, desde textos a imágenes o vídeos; simplemente con tener acceso a un ordenador se puede hacer pública sin problemas una determinada información, lo cual contrasta con la mayor dificultad de acceso a tradicionales medios de comunicación como la televisión, la radio o la prensa escrita. A esto se añade el hecho de que cada vez son más populares y manejables diferentes instrumentos de captación de la imagen y el sonido: destacadamente, las cámaras digitales y los teléfonos móviles, que sin dificultad alguna permiten realizar grabaciones. De todo ello se deriva que cada vez con más frecuencia son noticia casos de difusión de imágenes o vídeos en Internet, que de alguna manera comprometen la intimidad personal; asimismo, a veces se pone de relieve que en estos casos nos encontramos ante la comisión de delitos contra la intimidad. Sin embargo, lo cierto es que no todos los supuestos son iguales, ni en todos ellos se está verificando una de estas conductas

11. Cfr. ORTS / ROIG, *Delitos informáticos*, p. 28; RUEDA MARTÍN, *Protección penal de la intimidad*, pp. 62-63; MUÑOZ CONDE, F., *Derecho penal. Parte especial*, Tirant lo Blanch, Valencia 2007, p. 262; MORALES PRATS, en QUINTERO OLIVARES, *Comentarios*, pp. 410-411; ANARTE BORRALLO, E., "Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código penal", *Jueces para la democracia*, 2002, nº 43, p. 54.

delictivas. Centrándonos en esta problemática de difusión de imágenes en Internet, a continuación se hará una agrupación de las diferentes tipologías de casos para intentar ofrecer una solución a todos ellos.

En primer lugar, pueden agruparse todos aquellos **casos en que la toma de las imágenes ha sido consentida por el sujeto afectado, o ha sido realizada de forma lícita, y en cambio no hay consentimiento para su posterior difusión**.

Un ejemplo paradigmático de este conjunto de casos sería el de las *grabaciones consentidas* de vídeos de carácter sexual, que posteriormente son difundidas sin consentimiento de todos o de alguno de los participantes. Ya en alguna ocasión la jurisprudencia penal se ha ocupado de este tema, por ejemplo cabe citar la SAP Lleida 90/2004, sobre difusión de un vídeo sexual cuya grabación fue consentida por ambas partes, y que posteriormente fue difundido por uno de los dos participantes en el vídeo sin consentimiento del otro. El Tribunal entendió que la difusión del vídeo no podía considerarse delictiva a pesar de la ausencia de consentimiento, puesto que su obtención había sido lícita, se trataba de una grabación consentida por ambos participantes; por lo tanto, cuando no hay una previa captación ilícita de las imágenes, no puede ser delictiva su posterior difusión, ya que *el art. 197.3 CP exige que la revelación ha de referirse a datos ilícitamente obtenidos en el sentido del art. 197.1*[12].

Por lo tanto, este supuesto es similar a aquellos casos en que una persona difunde un vídeo sobre otro, cuando esa grabación ha sido consentida por el sujeto afectado. Cabe citar algún reciente caso que ha saltado a los medios de comunicación: la difusión en Internet de un vídeo sexual de una menor de edad, se supone que de forma no consentida, que había sido grabado en un parque con el consentimiento de la menor[13]. Al preguntarnos si en este supuesto se está cometiendo un delito contra la intimidad, la respuesta ha de ser negativa partiendo precisamente de lo dicho con respecto al caso anterior: dado que la obtención de la grabación no ha sido ilícita, sino que ha contado con el consentimiento del afectado, su posterior difusión no constituye delito contra la intimidad.

Cierto es que este caso tiene una particularidad: la persona afectada, consentidora de la filmación, era menor de edad, y aquí cabe plantearse hasta qué punto se considera válido el consentimiento de los menores de edad. Podemos acudir en primer lugar a la Ley orgánica 1/1996, de 15 de enero, de protección jurídica del menor; en su art. 4 se reconoce el derecho a la intimidad del menor y se establece lo siguiente: "se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales". De esta disposición legal se deduce que la eficacia del consentimiento de un menor de edad se ve limitada en relación con las utilizaciones de la imagen de los menores en medios de comunicación que puedan afectar a su reputación o a sus intereses. No obstante, esta norma

12. Cfr. MORALES PRATS, en QUINTERO OLIVARES, *Comentarios*, p. 429; ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, p. 145; RUEDA MARTÍN, *Protección penal de la intimidad*, pp. 94-95; HIGUERA GUIMERÁ, J.F., "El descubrimiento y la revelación de secretos", *Actualidad Penal*, 2002-3, m. 781.

13. Vid. El País 13-6-2007.

no nos sirve de gran ayuda en el caso señalado, puesto que se refiere a la ineficacia del consentimiento en relación con la difusión de la imagen en los medios de comunicación, no con respecto a la simple grabación de la imagen. Por lo tanto, el consentimiento del menor no sirve para autorizar la difusión de su imagen en los medios, pero nada se dice sobre su eficacia simplemente para permitir la filmación.

Cabría la posibilidad, entonces, de acudir a la regulación que el propio Código penal contiene sobre la eficacia del consentimiento, que está prevista en relación con los delitos de lesiones. Los arts. 155 y 156 CP determinan la atenuación de la pena en estos delitos cuando las lesiones son causadas con el consentimiento de la propia víctima; a tales efectos, el Código establece en qué casos se considera válida la prestación del consentimiento y por lo tanto puede dar lugar a este beneficio penológico. El art. 155 CP se manifiesta claramente: "no será válido el consentimiento otorgado por un menor de edad o por un incapaz".

No obstante, en relación con otras figuras delictivas en las que también puede resultar relevante el consentimiento se ha adoptado otra posición, en el sentido de llegar a admitir la capacidad de los menores de edad de prestar un consentimiento válido. Así ocurre en relación con los delitos relativos a la cooperación al suicidio, para cuya aplicación resulta necesario determinar si la muerte ha sido efectivamente un suicidio, es decir, que un sujeto ha consentido de forma voluntaria, con plena capacidad para ello, en provocarse su propia muerte. Al analizar si el suicida tiene efectivamente capacidad para consentir sobre la ejecución de la muerte, ante el silencio del Código penal al respecto se han propuesto diferentes teorías, y una de ellas es la que atiende a la capacidad natural de juicio, es decir, se trataría de examinar en el caso concreto si el sujeto tiene capacidad para comprender el sentido y trascendencia de la resolución de su voluntad[14]. Esta tesis, por lo tanto, no excluye de raíz la validez del consentimiento de los menores de edad: sería admisible afirmar que un menor puede consentir válidamente en causarse su muerte, si tiene la madurez suficiente para conocer la trascendencia de esa decisión en relación con el bien jurídico afectado, que es su propia vida.

A efectos de los casos que estamos tratando, sería admisible adoptar también esta tesis de la capacidad natural de juicio, y examinar en cada caso si el menor de edad tenía la madurez suficiente como para comprender el significado y trascendencia de la grabación de determinadas imágenes[15]. Se tratará, por lo tanto, de determinar la validez del consentimiento prestado; de este modo, siempre que se constate que la obtención de las imágenes ha sido válidamente consentida, su posterior difusión no puede integrar el delito del art. 197.3 CP. Si se determina que el menor no ha alcanzado el nivel de comprensión suficiente para consentir válidamente sobre estas actuaciones, ha

14. Vid. sobre la determinación de la capacidad de consentir en el ámbito de estos delitos de cooperación con el suicidio, VALLE MUÑIZ, J.M., en QUINTERO OLIVARES, *Comentarios*, p. 76; TOMÁS – VALIENTE LANUZA, C., *La cooperación al suicidio y la eutanasia en el nuevo Código penal (art. 143)*, Tirant lo Blanch, Valencia 2000, pp. 41 y ss; DÍEZ RIPOLLÉS, J.L., en DÍEZ RIPOLLÉS, J.L. / GRACIA MARTÍN, L. (coord.), *Comentarios al Código penal. Parte especial I*, Tirant lo Blanch, Valencia 1997, pp. 186 y ss.

15. De hecho, HIGUERA GUIMERÁ, "El descubrimiento y la revelación de secretos", m. 775, manifiesta que en el ámbito de los delitos contra la intimidad, el consentimiento del titular del bien jurídico exime de responsabilidad penal cuando precisamente acepta esa cesión de su intimidad; según este autor, debe entenderse que el consentimiento equivale a la capacidad natural de juicio.

de entenderse por consiguiente que la grabación fue inconsentida. Así, estaríamos ante aquellos casos en que existe una grabación no consentida y que posteriormente se difunde también sin consentimiento, cuyo tratamiento será analizado con posterioridad.

A pesar de la aparente claridad del art. 197 CP, que exige que los datos difundidos deben haber sido obtenidos con infracción del art. 197.1 CP, lo cierto es que el análisis de los casos concretos puede resultar sumamente confuso, y ello se aprecia en las resoluciones de los propios Tribunales. Así, cabe citar el caso de la SAP Almería 242/2005, que castiga como autor de un delito contra la intimidad a un sujeto que tenía en su poder unas fotos que una compañera de trabajo le había dado para que las revelase, y después del revelado difundió algunas de las fotos (en ropa interior) por correo electrónico. Si examinamos este caso, lo cierto es que nos encontramos con una situación de base semejante a la del caso del vídeo sexual consentido: si bien la difusión no es querida por la persona afectada, el acceso a las fotografías no ha sido realmente ilícito, ya que habían sido cedidas voluntariamente por su dueña.

El Tribunal aquí se centra en que, obviamente, las fotografías no habían sido cedidas para su publicación, sino sólo para su revelado. Sin embargo, lo mismo podríamos decir del caso del vídeo sexual: fue grabado para un uso particular, no para su futura divulgación. Por lo tanto, realmente en uno y otro caso puede afirmarse que el acceso a las imágenes no fue delictivo en el sentido del art. 197.1, ya que su captación fue consentida por la persona afectada. Evidentemente el consentimiento estaba limitado a unos determinados usos de las imágenes, lo cual obviamente determina la ilicitud de la difusión, pero únicamente desde un punto de vista no penal, sino como vulneración de la Ley orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Sin embargo, si no se puede constatar que el apoderamiento o captación de los datos o imágenes ha sido no autorizada, no cabrá aplicar el art. 197.3 a los comportamientos consistentes en su posterior difusión.

Este tratamiento de la difusión de imágenes obtenidas con consentimiento se puede aplicar también a los *casos en que tales imágenes son tomadas sin consentimiento del afectado pero de forma lícita*, porque la ley permite en determinados casos la captación de la imagen de una persona aunque no haya prestado consentimiento al efecto. De hecho, el art. 8 de la citada LO 1/1982 establece las siguientes autorizaciones:

1. No se reputará, con carácter general, intromisiones ilegítimas las actuaciones autorizadas o acordadas por la Autoridad competente de acuerdo con la Ley, ni cuando predomine un interés histórico, científico o cultural relevante.

2. En particular, el derecho a la propia imagen no impedirá:

a) Su captación, reproducción o publicación por cualquier medio cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público.

b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social.

c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza."

Por consiguiente, si una imagen tomada en el ejercicio de estas facultades que concede la Ley es posteriormente publicada, estaremos ante una conducta totalmente lícita, ya que incluso la ausencia de consentimiento en la propia captación de la imagen será irrelevante, puesto que la ley determina la licitud de estas filmaciones aun sin consentimiento del afectado.

Así, por ejemplo, podemos recordar el caso de una deportista estadounidense cuya imagen fue tomada en un acontecimiento deportivo y posteriormente publicada en Internet y, de forma absolutamente inopinada, la imagen alcanzó tal grado de éxito que empezó a circular por múltiples páginas y foros de Internet. Este hecho fue tan significativo que tuvo eco en los medios de comunicación, poniendo también de relieve el absoluto rechazo y disgusto de esta persona ante esa indeseada popularidad[16]. Sin embargo, tal difusión es totalmente lícita puesto que se trata de una imagen tomada en un acontecimiento de interés público y, por lo tanto, su captación y difusión están permitidas por la ley al margen del consentimiento del afectado[17].

También podríamos preguntarnos, incluso, sobre un reciente caso de agresión a una menor ocurrido en el metro, y que fue grabado por las cámaras de vigilancia colocadas en el vagón[18]. Esa grabación fue difundida repetidas veces a través de los medios de comunicación, reflejando no sólo a agresor y agredida, sino también a otras personas allí presentes que observaron el suceso sin actuar al respecto. Creo que resulta evidente que la difusión de estas imágenes no resulta delictiva puesto que, si bien ninguno de los sujetos filmados manifestaron su consentimiento ni en la grabación ni en la difusión del vídeo, la captación de tales escenas es lícita, puesto que se encuentra amparada por la Ley orgánica 4/1997, de 4 de agosto, que regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad Ciudadana en lugares públicos: tal y como establece esta ley, si se cumplen determinados requisitos está permitida la instalación de videocámaras en lugares públicos, por parte de Fuerzas y Cuerpos de Seguridad, con el fin de prevenir la comisión de infracciones relacionadas con la seguridad pública. Cuestión distinta es que la difusión de esta grabación constituya una infracción de la citada Ley orgánica, puesto que su art. 8 establece claramente un deber de confidencialidad sobre tales grabaciones por parte de las personas que tienen acceso a ellas en el ejercicio de sus funciones; como dice el art. 10 de la ley, la vulneración de este deber de sigilo puede determinar la exigencia de responsabilidad disciplinaria o también la comisión de una infracción en materia de protección de datos.

A continuación, pueden agruparse los **casos en que la captación de imágenes ni es consentida ni es lícita, y su posterior difusión tampoco cuenta con el consentimiento del afectado**.

---

16. Vid. El País 30-5-2007, Marca 31-5-2007.

17. Obviamente, se está tratando este caso con arreglo a la legislación española.

18. Vid. El País 25-10-2007.

Los ejemplos de este tipo de conductas son también numerosos, y pueden citarse algunos de ellos que frecuentemente acceden a los medios de comunicación: grabación de un vídeo sexual de una menor de edad en una habitación, sin su conocimiento, para posteriormente amenazarla con difundirlo por Internet[19]; grabación de un vídeo a un interno en un centro penitenciario, por parte de otros reclusos, para luego venderlo a algún medio de comunicación[20]; agresiones físicas o agresiones sexuales grabadas en teléfonos móviles y posteriormente difundidas en Internet[21]; grabación y difusión de vídeos de personas discapacitadas mientras alguien se está burlando de ellas[22], o también cuando están siendo objeto de una agresión[23].

En todos estos casos partimos de que ya la propia captación de las imágenes (no sólo su difusión) no es consentida; lo que se deberá hacer, por lo tanto, es comprobar que se verifican los requisitos del art. 197.3: se trata, fundamentalmente, de constatar que la actividad de obtención de los datos difundidos encaja en el art. 197.1 CP. *Sólo si se ha accedido a los datos o imágenes infringiendo este art. 197.1, se podrá considerar que su difusión es delictiva en el sentido del art. 197.3 CP.*

Recordemos entonces que la realización de la conducta típica del art. 197.1 requiere, ejemplificando con los casos que comentamos, que se haya producido una captación de imágenes ajenas, sin consentimiento del afectado y con intención de descubrir sus secretos o vulnerar su intimidad. No cualquier captación inconsentida de imágenes va a ser constitutiva de delito, sino que es necesario que sea realizada con el propósito de vulnerar la intimidad de la otra persona. Por este motivo, se excluiría del ámbito típico el apoderamiento de datos no conectados con la vida privada; en referencia concreta a la grabación de imágenes, precisamente por este motivo, y con el objetivo de restringir la intervención del Derecho penal a los supuestos más graves, *sólo se ha de considerar delictiva, por concurrencia de esta intención exigida en el tipo, la grabación de imágenes en lugares privados*[24], quedando fuera del ámbito típico la captación inconsentida de imágenes en lugares públicos, que constituirá en todo caso una vulneración de la LO 1/1982 de protección civil del derecho al honor, a la intimidad y a la propia imagen.

De este modo, los dos primeros ejemplos citados sí podrían dar lugar a la verificación del delito contra la intimidad recogido en el art. 197.3 CP, ya que los datos difundidos habían sido previamente obtenidos con infracción del art. 197.1. En el caso del vídeo sexual de la menor de edad, la captación de las imágenes había sido realizada sin su consentimiento y en lugar privado, con lo cual ya se estaría cometiendo el delito

---

19. Vid. El País 21-10-2007.

20. Vid. La Voz de Galicia 30-9-2006.

21. Vid. El País 24-11-2007, sobre la grabación de una agresión sexual y vid. también El País 30-6-2007 y La Voz de Galicia 2 y 3-11-2007, sobre grabación de agresiones físicas.

22. Vid. La Voz de Galicia 25-10-2007 y 25-11-2007.

23. Vid. La Voz de Galicia 16-12-2007.

24. Vid. así MORALES PRATS, en QUINTERO OLIVARES, *Comentarios*, p. 416; ROMEO CASABONA, *Los delitos de descubrimiento y revelación de secretos*, p. 96; RUEDA MARTÍN, *Protección penal de la intimidad*, p. 47; RUIZ MARCO, *Los delitos contra la intimidad*, pp. 70-71.

del art. 197.1; si quienes habían grabado el vídeo decidieran difundirlo posteriormente, estarían cometiendo el tipo agravado del art. 197.3. En el supuesto de la grabación de un vídeo entre reclusos de un centro penitenciario, la clave de la solución de este caso reside en la posible consideración del centro como un lugar privado: admitiendo tal posibilidad, puesto que realmente se trata de un lugar donde se desarrolla la vida personal de los que allí residen, la captación de las imágenes supondría la verificación del art. 197.1, y su posterior difusión la comisión del delito del art. 197.3.

Cuestión distinta son los demás ejemplos propuestos, puesto que por lo general estas grabaciones de agresiones o de discapacitados son efectuadas en la vía pública. Partiendo de la interpretación expuesta, el lugar de la grabación impide integrar tales supuestos en el ámbito típico del art. 197.1 CP, y por consiguiente, su posterior difusión no podría ser constitutiva del delito del art. 197.3; se trataría, entonces, de una difusión de imágenes personales que vulneraría la LO 1/1982 de protección civil de la intimidad, pero que no daría lugar a la verificación de un delito contra la intimidad.

De entrada puede resultar sorprendente la declaración de atipicidad de estas conductas; en todo caso, recordemos que nos estamos limitando a analizar la posible comisión de un delito contra la intimidad, que en estos supuestos realmente no se verifica porque así lo impide el Código penal. El art. 197 es claro: sólo cuando la obtención de las imágenes sea delictiva, se puede considerar también delictiva su posterior difusión; por consiguiente, al restringirse la intervención penal a los supuestos de captación de imágenes en lugares privados, es evidente que la filmación en lugares públicos no constituye infracción penal, y por lo tanto su posterior difusión sólo podrá ser constitutiva de un ilícito civil.

De todas formas, esto no implica afirmar la absoluta impunidad de los ejemplos propuestos. Recordemos que en algunos casos estamos ante agresiones físicas o sexuales, y esto ya implica una responsabilidad penal por *delitos de lesiones o de agresiones sexuales*, en cuya ejecución participan, en ocasiones, los propios sujetos que realizan la filmación.

Incluso si quien está realizando la filmación no participa en absoluto en la agresión, sino que simplemente se limita a grabar esta actuación ajena, cabría la posibilidad de considerar que comete *un delito de omisión del deber de socorro o un delito de omisión del deber de impedir delitos*. La primera infracción mencionada (art. 195 CP)[25] podría verificarse puesto que el sujeto en cuestión se halla delante de una persona desamparada en peligro manifiesto y grave, y cometería el delito si pudiendo auxiliarla sin riesgo, permanece a su lado con el único fin de grabar el hecho delictivo. La segunda de las infracciones (art. 450 CP)[26] se podría verificar si el sujeto, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impide la comisión del

25. Vid. sobre este precepto GARCÍA ALBERO, R., en QUINTERO OLIVARES, *Comentarios*, pp. 383 y ss; ARÁUZ ULLOA, M., *El delito de omisión del deber de socorro: aspectos fundamentales*, Tirant lo Blanch, Valencia 2006, pp. 340 y ss.

26. Vid. QUINTERO OLIVARES, G., en QUINTERO OLIVARES, *Comentarios*, pp. 1762 y ss; SOLÁ RECHE, E., *La omisión del deber de intervenir para impedir determinados delitos del art. 450 CP*, Comares, Granada 1999, pp. 99 y ss.

delito. Los evidentes puntos de conexión entre ambas figuras delictivas determinan que, con carácter general, exista un concurso de leyes entre los dos preceptos, considerándose preferente el art. 450 CP: así, si bien la conducta que estamos analizando encajaría de entrada en los dos tipos penales, se aplicaría este último precepto citado ya que contempla una omisión de carácter más específico[27]. No obstante, también cabría imaginar alguna situación en la que fuese posible aplicar ambos delitos: se trataría del caso en que el sujeto no impide la comisión del delito, y tras haber cesado esa concreta agresión, no socorre a la víctima desamparada[28].

Al margen de esta responsabilidad penal por ausencia de ayuda a la víctima, también cabría pensar si del propio comportamiento de grabación y difusión de imágenes se podría derivar otro tipo de responsabilidad fuera del marco de los delitos contra la intimidad. Ciertamente, tanto en estos casos de filmación de hechos delictivos, como en los supuestos de grabación de burlas a discapacitados, podría reconocerse una afectación al honor de las personas afectadas, derivada de la difusión de unas imágenes en las que están siendo víctimas de un delito o están siendo ridiculizadas. El *delito de injurias* (art. 208 CP)[29] abarca cualquier acción o expresión que lesiona la dignidad de la persona, menoscabando su fama o atentando contra su propia estimación. Por consiguiente, en estos ejemplos que estamos analizando es admisible reconocer que la difusión de este tipo de imágenes supone un claro atentado contra la dignidad personal. De hecho, podemos recordar la ya citada SAP Lleida 90/2004, sobre difusión de un vídeo sexual que había sido grabado previamente con consentimiento: el Tribunal absolvió al acusado de un delito contra la intimidad, ya que la obtención de las imágenes difundidas no había sido efectuada con infracción del art. 197 CP; sin embargo, condenó por comisión de un delito de injurias graves.

Y por último, ahondando en este aspecto de afectación a la dignidad y a la propia estima, en los casos más graves podríamos analizar incluso si se está verificando un *delito contra la integridad moral*. Esta infracción (art. 173.1 CP)[30] consiste en infligir a otra persona un trato degradante, menoscabando gravemente su integridad moral. La clave de interpretación de este precepto se halla en el contenido del bien jurídico "integridad moral", que podría definirse como el "derecho de toda persona a ser respetada en cuanto tal, no siendo sometida a procedimientos que, de modo vejatorio, degradante y humillante, la instrumentalicen, utilizándola como cosa y no como fin en sí misma considerada"[31]. Sería posible considerar, en algunos de estos casos, que se comete un

---

27. Cfr. SOLÁ RECHE, *La omisión*, p. 185.

28. Vid. HUERTA TOCILDO, S., *Problemas fundamentales de los delitos de omisión*, Madrid 1987, pp. 251-252; SOLÁ RECHE, *La omisión*, p. 185; GARCÍA ALBERO, en QUINTERO OLIVARES, *Comentarios*, p. 396.

29. Vid. QUINTERO OLIVARES, G. / MORALES PRATS, F., en QUINTERO OLIVARES, *Comentarios*, pp. 487 y ss; FERNÁNDEZ PALMA, R., *El delito de injuria*, Aranzadi 2001, pp. 131 y ss.

30. Vid. TAMARIT SUMALLA, J.M., en QUINTERO OLIVARES, *Comentarios*, pp. 261 y ss.

31. Vid. PÉREZ MACHÍO, A.I., *El delito contra la integridad del artículo 173.1 del vigente Código penal: aproximación a los elementos que lo definen*, Universidad del País Vasco 2005, pp. 230 y ss. Vid. también BARQUÍN SANZ, J., *Delitos contra la integridad moral*, Bosch, Barcelona 2001, pp. 50 y ss; MUÑOZ SÁNCHEZ, J., *Los delitos contra la integridad moral*, Tirant lo Blanch, Valencia 1999, pp. 19 y ss.

delito contra la integridad moral cuando un individuo es objeto de graves burlas y vejaciones, lo cual además es grabado y difundido por Internet; o incluso cuando un sujeto está siendo víctima de un delito particularmente grave, como determinadas lesiones o agresiones sexuales, y se procede a grabarlo en esa situación con el objetivo de incluirlo en páginas web con fines lúdicos.

De todas formas, al margen de las opciones mencionadas, cabe también reflexionar sobre si el concepto de intimidad podría experimentar una ampliación teniendo en cuenta las mayores posibilidades de exposición de la vida personal surgidas con el desarrollo de las nuevas tecnologías e Internet. De hecho, recordemos que ya en su momento los contornos del derecho a la intimidad fueron ampliados a raíz de la proliferación de las bases de datos informáticas: como se ha dicho con anterioridad[32], el Tribunal Constitucional configuró el "derecho al control de los datos personales" como parte del derecho a la intimidad, teniendo en cuenta la vulnerabilidad de esta información cuando es integrada en múltiples bases de datos informáticas de entidades públicas o privadas. Esta nueva faceta del derecho a la intimidad no sólo encontró protección a través de una normativa específica, que se centra en la LO 15/1999 de protección de datos personales, sino que incluso el Código penal procedió a castigar determinados atentados a los datos recogidos en ficheros automatizados, acogiendo de este modo la tutela de este aspecto del bien jurídico intimidad personal.

Lo cierto es que ya desde antiguo el Tribunal Constitucional reconoce, como parte del derecho a la intimidad, la posibilidad de decidir sobre la captación y difusión de la propia imagen. Consecuentemente, captar y difundir imágenes ajenas sin consentimiento del afectado supone una vulneración del derecho a la intimidad y así lo reconoce la LO 1/1982 de protección civil del derecho al honor, a la intimidad y a la propia imagen. Como se ha dicho, se restringe la intervención del Derecho penal a los casos en que la captación inconsentida de imágenes se realice en lugares privados.

No obstante, al igual que el legislador penal ofreció tutela al derecho de control de los datos personales, especialmente puesto en peligro por el desarrollo de las bases de datos informáticas, cabría pensar también en la posibilidad de proteger penalmente determinadas captaciones de imágenes, incluso en lugares públicos, teniendo en cuenta la especial vulnerabilidad de la imagen personal ante el desarrollo de las nuevas tecnologías e Internet. Ante la enorme facilidad de difusión de imágenes, propiciada por el desarrollo de la técnica, cabría preguntarse si este aspecto del derecho a la intimidad también merece tutela penal cuando las imágenes captadas, aun siendo en lugares públicos, comprometen de modo significativo la vida personal del sujeto. De todas formas, al margen de este posible debate sobre el significado de la intimidad en la era del rápido desarrollo de las nuevas tecnologías, no olvidemos que en todo caso la dignidad, el honor y en ocasiones incluso la integridad moral de las personas resultan afectados por la realización de las conductas que se han descrito con anterioridad.

---

32. Vid. supra epígrafe II.

BIBLIOGRAFÍA

ANARTE BORRALLO, E., "Consideraciones sobre los delitos de descubrimiento de secretos (I). En especial, el artículo 197.1 del Código penal", *Jueces para la democracia*, 2002, nº 43, p. 50.

ARÁUZ ULLOA, M., *El delito de omisión del deber de socorro: aspectos fundamentales*, Tirant lo Blanch, Valencia 2006.

BARQUÍN SANZ, J., *Delitos contra la integridad moral*, Bosch, Barcelona 2001.

DÍEZ RIPOLLÉS, J.L., en DÍEZ RIPOLLÉS, J.L. / GRACIA MARTÍN, L. (coord.), *Comentarios al Código penal. Parte especial I*, Tirant lo Blanch, Valencia 1997.

FERNÁNDEZ PALMA, R., *El delito de injuria*, Aranzadi 2001.

FERNÁNDEZ TERUELO, J.G., *Cibercrimen. Los delitos cometidos a través de Internet*, CCC 2007.

GARCÍA ALBERO, R., en QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007.

GÓMEZ NAVAJAS, J., *La protección de los datos personales*, Aranzadi 2005.

HIGUERA GUIMERÁ, J.F., "El descubrimiento y la revelación de secretos", *Actualidad Penal*, 2002-3, m. 767.

HUERTA TOCILDO, S., *Problemas fundamentales de los delitos de omisión*, Madrid 1987.

HUERTA TOCILDO, S. / ANDRÉS DOMÍNGUEZ, A.C., "Intimidad e informática", *Revista de Derecho penal*, 2002, nº 6, p. 11.

MATA Y MARTÍN, R.M., "La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías", *Revista Penal*, 2006, nº 18, p. 217.

MORALES PRATS, F., "Internet: riesgos para la intimidad", en AAVV, *Internet y Derecho penal*, CGPJ, Madrid 2001, p. 63.

– En QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007.

MORÓN LERMA, E., *Internet y Derecho penal: hacking y otras conductas ilícitas en la red*, Aranzadi 2002.

MUÑOZ CONDE, F., *Derecho penal. Parte especial*, Tirant lo Blanch, Valencia 2007.

MUÑOZ SÁNCHEZ, J., *Los delitos contra la integridad moral*, Tirant lo Blanch, Valencia 1999.

ORTS BERENGUER, E. / ROIG TORRES, M., *Delitos informáticos y delitos comunes cometidos a través de la informática*, Tirant lo Blanch, Valencia 2001.

PÉREZ MACHÍO, A.I., *El delito contra la integridad del artículo 173.1 del vigente Código penal: aproximación a los elementos que lo definen*, Universidad del País Vasco 2005.

QUINTERO OLIVARES, G., en QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007.

ROMEO CASABONA, C.M., "La protección penal de la intimidad y de los datos personales: los mensajes de correo electrónico y otras comunicaciones de carácter personal a través de Internet y problemas sobre la ley penal aplicable", en AAVV, *Estudios jurídicos del Ministerio Fiscal*, II – 2003, p. 73.

– "Los datos de carácter personal como bienes jurídicos penalmente protegidos", en ROMEO CASABONA, C.M. (coord.), *El cibercrimen: nuevos retos jurídico – penales, nuevas respuestas político – criminales*, Comares, Granada 2006, p. 167.

– *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia 2004.

RUEDA MARTÍN, M.A., *Protección penal de la intimidad personal e informática*, Atelier, Barcelona 2004.

RUIZ MARCO, F., *Los delitos contra la intimidad*, Colex, Madrid 2001.

SOLÁ RECHE, E., *La omisión del deber de intervenir para impedir determinados delitos del art. 450 CP*, Comares, Granada 1999.

TAMARIT SUMALLA, J.M., en QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007.

TOMÁS – VALIENTE LANUZA, C., *La cooperación al suicidio y la eutanasia en el nuevo Código penal (art. 143)*, Tirant lo Blanch, Valencia 2000.

VALLE MUÑIZ, J.M., en QUINTERO OLIVARES, G. (dir.), *Comentarios a la parte especial del Derecho penal*, Aranzadi 2007.