

# LA PROTECCIÓN PENAL DEL DERECHO A LA INTIMIDAD

Javier Zaldívar Robles

Profesor Asociado de Derecho penal  
Universitat Jaume I de Castelló

**Sumario:** 1. Introducción. 2. El derecho a la intimidad. 2.1 Aproximación conceptual. 2.2. Concepto de intimidad y otros términos asimilados. 2.3. Régimen jurídico del derecho a la intimidad. 2.4. La intimidad del siglo XXI. 2.5. Análisis de noticias actuales. 3. Marco jurídico de protección del derecho a la intimidad: 3.1. Espacio europeo. 3.2. Ámbito constitucional. 3.3. Ámbito civil. 4. La protección administrativa del derecho a la intimidad: la Agencia de Protección de Datos. 4.1. Normativa reguladora. 4.2. Análisis de algunas resoluciones de interés sobre la tutela de la intimidad de las personas físicas. 4.3. Problemática en la protección del derecho a la intimidad de las personas jurídicas. 4.4. La garantía del derecho a la intimidad ante los órganos judiciales. 5. La Protección penal del derecho a la intimidad en el Código penal: especial referencia con las nuevas tecnologías. 6. Conclusiones.

## 1. INTRODUCCIÓN

Hace más de dos años, el 28 de febrero de 2014, el diario *El País* publicó en su versión digital una noticia con este titular: «Inteligencia británica interceptó webcams de usuarios de yahoo». En el cuerpo de la información, podía leerse lo siguiente: «Durante los primeros seis meses de 2008, un programa del GCHQ (Government Communications Headquarters) recopiló planos de conversaciones en video de más de 1,8 millones de titulares de cuentas de Yahoo!, afirmó *The Guardian* citando documentos filtrados por el exanalista estadounidense Edward Snowden, refugiado en Moscú. Entre esas imágenes, figuran “una cantidad sustancial de comunicaciones explícitamente sexuales”, añadió el diario en el artículo publicado en su edición en internet».

En la actualidad convivimos diariamente con noticias como el espionaje entre Estados, el espionaje entre multinacionales o, descendiendo a lo cotidiano, invasiones en la esfera privada entre particulares, conductas invasoras

y lesivas para cualquier ciudadano. Expresiones como *sexting*, *grooming*, *pharming*, *phishing*, *hacker*, *cracker* o el reciente *leakednude* han pasado a formar parte de nuestra preocupación cotidiana.

El uso de las nuevas tecnologías y de las redes sociales está provocando una creciente sensación de inseguridad en la privacidad de las personas. Así las cosas, la sociedad debe plantearse exigir a los poderes públicos una regulación más proteccionista y garantista del derecho a la intimidad. Esta nueva concienciación social ya está obteniendo resultados: por ejemplo, la presión ejercida por sociedad americana ha dado como resultado la reciente aprobación en el Senado de los EEUU la reforma de la polémica Patriot act<sup>1</sup> y, consecuentemente, el recorte de poderes a la NSA. No obstante, conviene señalar que una protección eficaz de nuestra intimidad nace en el propio individuo y en cómo gestiona las barreras de seguridad previstas.

En este artículo pretendo abordar de manera sucinta los distintos ámbitos de protec-

ción del derecho a la intimidad en nuestro ordenamiento jurídico, profundizando en el análisis del Derecho punitivo.

## 2. EL DERECHO A LA INTIMIDAD

### 2.1. APROXIMACIÓN CONCEPTUAL

Debemos al escritor Milan Kundera esta excelente reflexión: «La persona que pierde su intimidad, lo pierde todo». Me planteo al respecto si hemos perdido «todo» en la sociedad actual. Con frecuencia se debate sobre la «intimidad», pero realmente debemos preguntarnos qué es el derecho a la intimidad y qué características o parámetros definen su contenido. No es tarea fácil perfilar un concepto estable y pacífico del derecho a la intimidad, habida cuenta de que se trata de un bien jurídico que va mutando con el transcurso del tiempo y los cambios sociales.

El punto de partida hay que fijarlo en el individuo. Como señala Herrero Tejedor, los derechos de la personalidad (el derecho a la intimidad, entre otros) hay que radicarlos en la propia persona, puesto que «todo el derecho existe por causa del hombre, y es este el sujeto primario e indefectible tanto del derecho privado como del público, los derechos de la personalidad son innatos y se adquieren por el simple hecho del nacimiento (artículo 32 CC)»<sup>2</sup>. Por este motivo, no es casualidad que, en su artículo 10.1, nuestra Carta Magna disponga que la dignidad de la persona, los derechos inviolables que le son inherentes y el libre desarrollo de la personalidad conforman el fundamento del orden político y de la paz social.

Tradicionalmente, el derecho de intimidad se identificaba con el «derecho de reserva» o el «derecho a la vida privada». Las facultades jurídicas ostendadas por el titular del derecho le permitían oponer cualquier tipo de exclusión o barrera de su ámbito familiar o personal frente a terceros. Este enfoque clásico del derecho a

la intimidad lo ubicaba como un apéndice del derecho al honor.

Con la vertiginosa evolución tecnológica a finales del siglo XIX, y de la mano de la obra de Warren y Brandeis<sup>3</sup>, nace en la cultura anglosajona el derecho a la *privacy*, un nuevo derecho autónomo dentro de la familia de los derechos de la personalidad. Como también hizo el profesor Fayos en una de sus obras<sup>4</sup>, merece la pena rescatar aquí un clarividente fragmento del artículo de ambos autores: «De la convivencia —más bien de la necesidad— de tal protección, creemos que no puede haber ninguna duda. La prensa está sobrepasando en todas las direcciones los límites obvios de la propiedad y de la decencia [...] y el hombre, bajo la refinada influencia de la cultura, se ha vuelto más sensible hacia la publicidad, de manera que la soledad y la intimidad se han hecho más esenciales para el individuo». Quisiera poner de relieve que esta reflexión la realizaban a finales del siglo XIX un abogado de prestigio (Warren) y su exsocio (Brandeis), que a la postre fue nombrado juez del Tribunal Supremo americano, y que en el texto destacaban la necesidad de «soledad e intimidad» por tratarse de una parte esencial para el ser humano. Sin duda, 125 años después de la publicación de dicho artículo el contenido del mismo es perfectamente aplicable y exigible en la actualidad.

Con el nacimiento del *right to privacy* se han ido forjando nuevos mecanismos de defensa o tutela de la intimidad. En primer lugar, es la persona como titular del derecho a la intimidad la que debe imponer un control sobre sus datos personales que circulan en la sociedad tecnológica —es lo que se conoce hoy en día como el *habeas data*—. Este control o gestión de los propios datos se realiza mediante el derecho de acceso a los bancos de datos y los derechos de rectificación o de cancelación. Por lo tanto, la cultura anglosajona de la *privacy* interpreta el derecho a la intimidad como una esfera de libertad con proyección social que la persona ejercita con plena libertad y control. En segundo lugar, impera un mayor control

institucional de todo lo que rodea al mundo de las nuevas tecnologías (así nació en España la Agencia de Protección de Datos).

Ubicados ya en la actualidad, resulta patente que hoy en día Internet es un mundo «virtual» en el que se relacionan las personas, las instituciones (públicas o privadas), los partidos políticos y todo tipo de entes y organismos. Estas relaciones *inter partes* se gestionan a través de correos electrónicos, cibernavegación, compras, apuestas, contrataciones *on line*, etc. Dentro de este «mundo virtual» se realizan numerosas actividades que ponen en grave peligro la intimidad de los ciudadanos a nivel global, configurándose un nuevo estatus bautizado como «el ciudadano de cristal o transparente»<sup>5</sup>.

En los últimos años, los tribunales y otros operadores jurídicos han advertido que se está sobrepasando con creces el límite del derecho a la información o la libertad de expresión en detrimento del derecho a la intimidad o privacidad del individuo. Esta preocupación ha quedado recientemente plasmada en la sentencia del Tribunal Europeo de Derechos Humanos que ha resuelto a favor de un ciudadano español que ejercitaba su «derecho al olvido» contra la plataforma Google. Profundizaré más adelante en esta importante resolución.

## 2.2. CONCEPTO DE INTIMIDAD Y OTROS TÉRMINOS ASIMILADOS

En la segunda acepción del término, el diccionario de la RAE define la «intimidad» como la «zona espiritual íntima y reservada de una persona o grupo, especialmente de una familia»<sup>6</sup>. La idea que subyace es que nos encontramos en la zona más interna y espiritual de una persona, en un espacio que debe ser custodiado con recelo para evitar que llegue al conocimiento general de terceras personas; se trata, en fin, de una parcela privada y sometida a la voluntad única y exclusiva de su titular y no del público.

Algún sector de la doctrina y también el TC han asumido una concepción subjetiva de la intimidad que la considera como un espacio íntimo bajo el prisma no de pautas sociales o culturales, sino desde un enfoque personal, es decir, de lo que cada sujeto entienda como íntimo<sup>7</sup>. En la jurisprudencia consolidada de los años 90, el Tribunal Constitucional consideraba que el derecho a la intimidad personal implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario para mantener una calidad mínima de vida humana<sup>8</sup> según las pautas de nuestra cultura. Recordemos que esta caracterización se aproxima al concepto que defendían Warren y Brandeis en su artículo doctrinal sobre el *right to privacy* a finales del siglo XIX<sup>9</sup>.

Algunos términos asimilados a la intimidad son los siguientes: privado, confidencial, reservado, personal, esencial u oculto. Aunque estos son distintos a la acepción de la intimidad arriba reproducida, no es menos cierto que se utilizan en un lenguaje cotidiano o vulgar como sinónimos<sup>10</sup>. Asimismo, nos encontramos con la utilización indistinta de los términos intimidad y vida privada. Para Rebollo Delgado<sup>11</sup>, el concepto de vida privada es muy amplio y genérico, y da cabida a toda aquella información que el titular no desea que se conozca de manera general por el resto de personas.

## 2.3. RÉGIMEN JURÍDICO DEL DERECHO A LA INTIMIDAD

La protección de la intimidad no es una empresa fácil. En la sociedad contemporánea, el núcleo personal y familiar íntimo se ha vuelto más vulnerable. En muchos hogares, cualquier miembro puede acceder a las redes sociales a partir de temprana edad con un ordenador portátil, una *tablet* o un *smartphone*, y tiene capacidad de navegar, chatear o «tuitear» información, fotos o vídeos. Todo este volcado de datos en el mundo virtual se realiza en la mayoría de ocasiones por el individuo sin adoptar medidas de

protección y control en relación con las personas que pueden acceder a dicha información, lo que deriva en una pérdida de control de esos datos personales, que quedan al alcance de cualquier persona que los consiga en la red.

En mi opinión, coincidente con la de la mayoría de los expertos en la materia, la protección más importante del derecho a la intimidad parte de una conducta preventiva del propio usuario de la red. Es necesario transmitir una mayor concienciación e información a los jóvenes (y a los no tan jóvenes) de los riesgos inherentes al volcado de información de naturaleza sensible o íntima en las redes sociales. El usuario de esas plataformas debe ser diligente y activar todos los mecanismos de control y seguridad, así como establecer los máximos filtros para evitar o, cuando menos, dificultar que cualquier persona desconocida o «no deseada» tenga acceso a esa información privada o personal.

En la actualidad, la protección del derecho a la intimidad se regula en dos escenarios jurídicos distintos. El primero es el marco legal europeo, habida cuenta que España, como Estado miembro de la Unión Europea, queda sometida al cumplimiento de las Directivas que provienen del órgano legislativo de Bruselas. El segundo es el ordenamiento jurídico interno o nacional, dividido a su vez en las protecciones que brindan los órdenes constitucional, civil, administrativo y penal.

Interesa traer a colación algunos movimientos que están emergiendo como consecuencia de la concienciación social de la necesidad imperiosa de proteger la información e intimidad personal, como la conocida «Lista Robinson»<sup>12</sup>. Esta lista de exclusión publicitaria —gestionada por Adigital y de carácter gratuita— es un servicio a través del cual los ciudadanos se inscriben porque no desean recibir publicidad de entidades con las cuales no mantienen ni han mantenido ningún tipo de relación comercial.

Finalmente, quisiera poner de relieve la reciente normativa<sup>13</sup> en materia de protección de

los consumidores y usuarios destinada a prohibir que a partir de ciertas horas y días concretos (festivos o fines de semana) se realicen llamadas con fines comerciales o de publicidad (las llamadas conocidas como «spam telefónico»), dado que estas merman la calidad de la vida personal y familiar de quien las recibe, y, por extensión, perturban la intimidad de los consumidores y usuarios.

#### 2.4. LA INTIMIDAD DEL SIGLO XXI

No existe una postura doctrinal pacífica en torno al contenido del derecho a la intimidad. El motivo es obvio: la intimidad puede ser percibida de forma distinta y con límites diferentes en distintos momentos de la vida de las personas. También se asume por algunos individuos que su derecho a la intimidad queda reducido cuando ostenta alguna profesión o cargo que le coloca en el punto de mira de todos los objetivos de los medios de comunicación y, por ende, de la opinión pública.

El concepto de intimidad ha ido mutando a lo largo de la historia. Al respecto, Giddens<sup>14</sup> señala que la intimidad configuró un binomio con la sexualidad de las personas a lo largo de la evolución de la sociedad. En su obra sostiene que el amor romántico (cuyo nacimiento se ubica a finales del siglo XVIII), que separa conceptualmente del *amour passion*, ya suscitaba el debate conceptual sobre la intimidad, ya que se entendía que esta era incompatible con la lujuria y con la sexualidad terrenal (cualidades que se desarrollaban de forma más pasional o animal en el *amour passion*)<sup>15</sup>. Asimismo, insiste en que la intimidad ha entrado en una nueva fase histórica, que es la que nos afecta hoy en día y que denomina la «democratización de la vida personal»<sup>16</sup>. Una sociedad democrática debe sostenerse en el principio de la autonomía, entre otros, del cual debe gozar todo individuo para su desarrollo personal y familiar.

Debo concluir apuntando que la preocupación por proteger el derecho de intimidad

es una realidad que se encuentra sobre la mesa de debate en la UE. Las instituciones europeas son conscientes de la necesidad de aprobar un Reglamento ajustado a los tiempos actuales sobre el tratamiento de los datos privados y sensibles de los ciudadanos. Hasta la fecha, sigue vigente la Directiva 1995/46/CE en materia de protección del tratamiento de los datos de las personas físicas y su circulación, sin duda ya obsoleta si tenemos en cuenta la rapidez con la que avanzan las nuevas tecnologías.

## 2.5. ANÁLISIS DE NOTICIAS ACTUALES

El prestigioso periódico alemán *Die Welt* publicaba el artículo «Maas warnt vor dem gläsernen Autofahrer»<sup>17</sup>. En una entrevista concedida al citado medio por el ministro de Justicia de Alemania, Hr. Heiko Maas, el político criticaba de forma contundente los medios tecnológicos utilizados en los vehículos modernos (conocidos como *smart cars*). A través de los *smart cars* se recopila todo un elenco de datos e información como la ubicación del vehículo en todo momento y hora (GPS), la velocidad media, máxima y mínima de circulación, el número de personas que ocupan el vehículo e incluso en qué posición, además de otros datos que también se recogen en una central de datos del vehículo, datos que son posteriormente almacenados en un disco duro del ordenador del turismo. A la luz de todo ese compendio de información, el ministro alemán afirma con notoria preocupación que se podría estar vulnerando seriamente el derecho de intimidad de los alemanes (*Persönlichkeitrechts*), quienes, no lo olvidemos, consideran su automóvil como una extensión de su esfera privada e íntima. El debate que se está suscitando en la opinión pública gira alrededor de diversas cuestiones: ¿a quién pertenecen todos esos datos recogidos en el ordenador del vehículo?, ¿quién ostenta la legitimación o titularidad de esos datos?, y, finalmente, ¿pueden ser utilizados estos datos por los poderes públicos como prueba de cargo en un procedimiento judicial contra el propio conductor o propietario del vehículo? Pode-

mos comprobar que no son cuestiones baladíes y que en la actualidad existe una profunda preocupación en la sociedad germana sobre la necesidad de proteger de forma más eficaz y eficiente la vida privada (*die Privatsphäre*) desarrollada dentro del vehículo particular.

Otra de las noticias destacables ha sido la voz de alarma lanzada por los operadores jurídicos y por expertos informáticos respecto a la vulnerabilidad de la plataforma WhatsApp. En el periódico *El País* se publicaba el artículo «Whatsapp, falso testigo»<sup>18</sup> en el que dos ingenieros informáticos españoles expertos en ciberseguridad afirmaban que habían podido quebrar el código de dicha plataforma para modificar el remitente de un mensaje. De esta forma, dejaban en entredicho la «seguridad» del servicio de mensajería que utilizan más de 500 millones de usuarios, así como la inseguridad que se origina cuando en sede judicial se utiliza como material probatorio mensajes enviados desde una plataforma donde puede ser «manipulable» el remitente —fácilmente suplantable por otra persona—, con las consecuencias jurídicas que esto conlleva si hablamos de posibles infracciones penales como delitos de extorsión, amenazas graves, o posibles infidelidades conyugales inexistentes, pero lanzadas por quien suplanta falsariamente al remitente. En reciente sentencia<sup>19</sup>, el Tribunal Supremo ha advertido de que no se aceptará como prueba válida cuando la autenticidad de las conversaciones en sede virtual sea puesta en entredicho por la otra parte y que la carga probatoria recaerá sobre quien pretenda hacerlas valer, que deberá corroborar dicha prueba mediante un perito experto en la materia que acredite su veracidad.

Es claro, por lo tanto, como ya denunciaba Bueno Mata<sup>20</sup>, que «la Justicia no está preparada, no existe a día de hoy la figura del Juez 2.0». Esta afirmación la sostiene con el argumento de que la Ley de Enjuiciamiento Civil es del año 2000 y la plataforma Whatsapp se creó en el año 2009).

Al hilo de lo expresado por Bueno Mata, en el ámbito del Derecho procesal penal conviene

reseñar que la decimonónica Ley de Enjuiciamiento Criminal ha sido recientemente modificada mediante la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológicas y por la Ley 42/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para la agilización de la justicia penal y el fortalecimiento de las garantías procesales. Esta reciente reforma de la Ley de Enjuiciamiento Criminal persigue adecuar las nuevas investigaciones de delitos tecnológicos por parte de las fuerzas y cuerpos de seguridad a la normativa europea, así como a la interpretación protectora y limitadora de los derechos fundamentales en juego que venía siendo elaborada jurisprudencialmente debido a la obsolescencia de la norma procesal.

Finalmente, quisiera reseñar que uno de los ámbitos que más inquieta a los Estados y a las empresas es la ciberseguridad y, en concreto, la protección de los datos de carácter íntimo y sensible que pueden ser captados por los *hackers*. Hace apenas unos meses se publicaba la noticia titulada «España busca hackers de los buenos»<sup>21</sup>, texto que incidía en la problemática actual y global del robo de información de datos en Internet. Según la periodista que firma la noticia, España es el segundo país más atacado (después de EE. UU.) y concentra el 20% de los ciberataques internacionales, lo que denota la gravedad del asunto y la constante puesta en peligro de la intimidad de millones de ciudadanos; una muestra de ello es la repercusión internacional originada por la filtración de los datos de filiación de muchos clientes de la agencia Ashley Madison.

### 3. MARCO JURÍDICO DE PROTECCIÓN DEL DERECHO A LA INTIMIDAD

#### 3.1. ESPACIO EUROPEO

España, como cualquier Estado miembro perteneciente a la UE, se encuentra sujeto a la

normativa que dimana de los órganos legislativos de la Unión. Ya en el artículo 8 del Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales (Roma, 1950) se regula *the right to the respect for private and family life*, es decir, el derecho a la vida privada y familiar, que engloba la intimidad del domicilio y la inviolabilidad de la correspondencia y establece límites a la injerencia por parte de los poderes públicos o de terceros.

A partir de los años 80, en la entonces denominada Comunidad Económica Europea nacía la preocupación por el derecho a la intimidad de sus ciudadanos y por el tratamiento que debía realizarse de la información de contenido sensible del ámbito de la intimidad. La primera norma europea dictada fue el Convenio núm. 108 del Consejo, del año 1981, que regulaba la protección de las personas en lo concerniente al tratamiento automatizado de datos de carácter personal e incidía, sobre todo, en el derecho al respeto de la vida privada. Con la Directiva 95/46/CE (vigente en la actualidad) del Parlamento y el Consejo, de 24 de octubre de 1995 (en adelante, «la Directiva»), la UE perseguía mejorar en la protección del derecho a la intimidad de sus ciudadanos. Otra de las notas a destacar de la Directiva es la remisión a los Estados miembros para que estos regularan los recursos y sanciones a imponer por las infracciones cometidas contra la normativa, así como la propuesta de que se regulara un recurso de naturaleza administrativa ante las autoridades, lo que en nuestro ordenamiento conllevó a la creación de la Agencia Española de Protección de Datos.

Sin ánimo de ser exhaustivos, debemos citar otras normas como la Directiva 2002/58/CE del Parlamento Europeo y el Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201, de 31 de julio de 2002), modificada por las Directivas 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con

la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (DO L 105, de 13 de abril de 2006) y 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas y el Reglamento (CE) núm. 2006/2004 sobre la cooperación en materia de protección de los consumidores (DO L 337, de 18 de diciembre de 2009) y la Decisión Marco 2005/222/JAI del Consejo de la UE, de 24 de febrero de 2005, de protección de la seguridad informática por parte de los Estados miembros.

Por último, dada su actualidad y relevancia, no puedo obviar el análisis de la sentencia de fecha 13 de mayo de 2014 dictada por el Tribunal de Justicia de la Unión Europea (Gran Sala)<sup>22</sup>, que abordó una cuestión prejudicial planteada por la Audiencia Nacional con base en el artículo 267 TFUE y resolvió un caso sobre el derecho al olvido ejercitado por un ciudadano español que demandó a las compañías Google Spain, S.L. y Google Inc. Cabe destacar de la resolución los siguientes argumentos: i) la actividad realizada por los motores de búsqueda para hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de terceros internautas se califica como tratamiento de datos personales y, por lo tanto, el gestor de estos motores es el responsable de dicho tratamiento; ii) se considera tratamiento de datos personales en el marco de actividades de un establecimiento del responsable de dicho tratamiento, en un territorio de un Estado miembro aun cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o filial destinada a garantizar la promoción y la venta de espacios publicitarios por el motor de búsqueda y cuya actividad tiene como destinatarios los habitantes de ese Estado miembro; iii) el gestor de un motor de búsqueda está

obligado a eliminar de la lista de resultados obtenida tras una búsqueda realizada a partir del nombre de una persona con vínculos a páginas web, publicación de terceros que contenga información de esa persona, aunque en dichos vínculos o web su publicación fuera lícita; iv) en relación con el derecho al olvido, el Tribunal resuelve a favor del interesado y le faculta a exigir la retirada de una información relativa a su persona cuando no se ajuste a la realidad y le ocasione un perjuicio al salir vinculada a su nombre en una lista de resultados obtenida tras la búsqueda, todo ello por encima de otros intereses que puedan verse afectados como los rendimientos económicos del gestor de motor de búsqueda o el interés del público en general de acceder a esa concreta información sobre esa persona.

No obstante, pese a los argumentos detallados, el Tribunal deja abierta la excepción para aquellos supuestos en que la persona física tenga proyección pública y, por lo tanto, la injerencia esté justificada por el interés «preponderante» del público en disponer del acceso a tal información.

### 3.2. ÁMBITO CONSTITUCIONAL

La regulación del derecho a la intimidad se encuentra ubicada en el artículo 18 CE como un derecho fundamental y está desarrollada en la LO 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (en adelante, LO 1/82). Asimismo, debe citarse la LO 15/1999, de 13 de diciembre, de protección de datos de carácter personal, por su afectación al derecho de la intimidad de las personas, y la LO 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, complementaria a la Ley 11/2002, de 7 de mayo, que reglamenta el funcionamiento del Centro Nacional de Inteligencia y pretende establecer las bases de un control judicial (concretamente por un magistrado del Tribunal Supremo) de las actividades desplegadas por el CNI siempre que se vean afectados

los derechos fundamentales del artículo 18.2 y 3 CE (la inviolabilidad del domicilio y el secreto de las comunicaciones)<sup>23</sup>.

El perfil del derecho a la intimidad —en constante conflicto, como es sabido, con el derecho fundamental de libertad de información— ha ido moldeándose por la evolución jurisprudencial del Tribunal Constitucional. Hasta no hace muchos años, el TC venía otorgando una prevalencia casi automática a la libertad de expresión en detrimento de la intimidad de aquellas personas de naturaleza pública. No obstante, en los últimos dos años (2013-2014) el máximo garante e intérprete de los derechos fundamentales ha dictado algunas sentencias en las que se percibe una posición más proteccionista del derecho de la intimidad de las personas, aun tratándose de personalidades públicas, siempre y cuando la información publicada no goce del interés general de la ciudadanía. Dado que en el presente artículo no pretendo analizar el orden jurídico, recomiendo la lectura y análisis de una de estas últimas sentencias publicadas por el Tribunal Constitucional<sup>24</sup>.

### 3.3. ÁMBITO CIVIL

Como he adelantado, en el orden civil la norma que regula y protege el derecho de la intimidad es la LO 1/1982. En el epígrafe anterior afirmaba que la intimidad es un derecho fundamental que se reconoce en el apartado primero del artículo 18 CE (junto al derecho a la propia imagen), y es pacífica la doctrina constitucional en considerarlo un derecho autónomo<sup>25</sup> respecto a los derechos recogidos en los apartados segundo (la inviolabilidad del domicilio), tercero (secreto de las comunicaciones) y cuarto (el *habeas data* o derecho de los datos informáticos) del mismo precepto.

Considero interesante señalar que la LO 1/82 es la norma aplicable a los efectos de facilitar los criterios para calcular la indemnización civil por vulneración de los derechos que

protege cuando estos son perseguidos y castigados en un procedimiento penal.

Cabe finalmente reseñar que, pese a las habituales fricciones entre el TS y el TC (como muestra, remito a la lectura de la STC 7/2014 de 27 de enero), no podemos soslayar la interpretación del derecho a la intimidad realizada por la Sala 1ª del Tribunal Supremo<sup>26</sup>, en relación con unos comentarios emitidos en un programa de gran audiencia en nuestro país, *El intermedio*; el presentador de este espacio vertió afirmaciones de contenido injurioso y denigrante respecto a una persona pública, y resaltó su posible homosexualidad. A modo de resumen, las argumentaciones del TS fueron las siguientes: i) en relación con la ponderación de los derechos fundamentales en colisión (el derecho a la intimidad y el honor *vs.* el derecho a la información y expresión), el libre ejercicio del derecho a la libertad de expresión, al igual que el de información, garantiza un interés constitucional relevante, pero encuentra un límite constitucionalmente reconocido en el derecho a la intimidad de las personas; ii) en relación con la «doctrina del reportaje neutral», rechaza su aplicación al entender que el programa objeto de controversia no tienen el amparo de tal doctrina, dado que los comentarios vertidos por el presentador del programa fueron propios y de naturaleza injuriosa [a los que ya procedían de una tercera persona]; iii) no existe un amparo constitucional al derecho al insulto; iv) la ponderación del interés público del asunto tratado era escaso. El Tribunal señala que no debe confundirse la noticia que pueda tener una trascendencia o interés público con otra de carácter privado y personal que pueda interesar a un cierto público, ávido de este tipo de información ajena como mero entretenimiento; v) finalmente, la resolución aborda los comentarios jocosos sobre la inclinación sexual de una persona y explícita de qué manera pueden lesionar la intimidad del demandante: «Con respecto a las expresiones relativas a la condición sexual del demandante, la doctrina de esta Sala y del

Tribunal Constitucional han declarado que la atribución de una determinada condición sexual sin consentimiento y en contra de la conducta públicamente conocida, puede ser formalmente lesiva del derecho a la intimidad cuando aparece desvinculada de cualquier finalidad informativa y del objetivo de formación de una opinión pública libre (SSTS 03-03-2003 en RC 2160/1997, 22-06-2010 en RC 1902/2007 y 28-06-2012 en RC 591/2011; STC 77/2009 FJ 4) [...] porque a menudo, el propósito burlesco, *animus iocandi*, se utiliza precisamente como instrumento del escarnio (SSTC 176/1995 FJ 5 y 23/2010 FJ 5)».

## 4. LA PROTECCIÓN ADMINISTRATIVA DEL DERECHO A LA INTIMIDAD: LA AGENCIA DE PROTECCIÓN DE DATOS

### 4.1. NORMATIVA REGULADORA

La Agencia Española de Protección de Datos es una de las instituciones que conforman lo que la doctrina denomina «garantías institucionales», y coexiste con otras instancias de tutela de los derechos fundamentales como el Ministerio Fiscal, el Defensor del Pueblo, o los juzgados y tribunales ordinarios, sin olvidar del procedimiento del recurso de amparo ante el Tribunal Constitucional.

La AEPD viene regulada por la siguiente normativa: i) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; ii) Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; iii) Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.

### 4.2. ANÁLISIS DE ALGUNAS RESOLUCIONES DE INTERÉS SOBRE LA PROTECCIÓN DE LA INTIMIDAD DE LAS PERSONAS FÍSICAS

A continuación analizo dos resoluciones recientes de la AEPD que suscitan algún interés jurídico en lo que concierne al derecho a la intimidad.

– Denegación del derecho de cancelación a un paciente respecto a sus datos de un fichero de centro médico<sup>27</sup>:

En este caso, el reclamante ejercitó su derecho de cancelación ante la entidad reclamada y su solicitud obtuvo la respuesta legalmente exigible;

«En virtud del artículo 33.1 del RLOPD relativo a la denegación de los derechos de rectificación y cancelación, determina: La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos. En consecuencia, la cancelación solicitada está basada en la supresión de los datos personales necesarios para la gestión de la relación contractual existente entre reclamante y reclamado por lo que no procede la cancelación solicitada (...) el derecho fundamental a la protección de datos no resulta absoluto, ni prevalece en cualquier caso ante otros intereses o derechos dignos de protección, como la propia jurisprudencia constitucional establece [...]».

Por todo lo anteriormente expuesto, la cancelación de los datos contenidos en las historias clínicas relativos a la salud del individuo y cuya consulta resulte adecuada para preservar su salud, deberán conservarse durante el tiempo adecuado a cada caso, obviamente sustentándose en el criterio médico, y no procede cancelar dichos datos cuando pudiera perju-

dicarse la salud futura del paciente al que se refieren los mismos.

– Denegación de protección a un notario por vulneración del derecho a la intimidad por la Dirección General de los Registros y del Notariado. Archivo de las actuaciones por falta de competencia de la AEPD<sup>28</sup>.

En este caso se abordó la denuncia interpuesta por un registrador de la propiedad a la DGRN por la incorporación a la resolución de fecha 0000, que resolvía el recurso gubernativo interpuesto contra la calificación negativa efectuada por el denunciante con la utilización de expresiones y valoraciones merecedoras de un procedimiento sancionador.

La AEPD se acogió a la doctrina establecida en la STC 292/2000, de 30 de noviembre, en la que el Tribunal Constitucional<sup>29</sup> configura el derecho fundamental a la protección de datos de forma autónoma respecto al derecho a la intimidad y señala, en su FJ 6: «La función del derecho fundamental a la intimidad del art. 18.1 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad [...] En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno [...], es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos [...]. De este modo, el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su

objeto no es solo la intimidad individual que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal [...]. Pero también el derecho fundamental a la protección de datos posee una segunda peculiaridad que lo distingue de otros, como el derecho a la intimidad personal y familiar del art. 18.1 CE. Dicha peculiaridad radica en su contenido, ya que a diferencia de este último, que confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima de la persona y la prohibición de hacer uso de lo así conocido, el derecho a la protección de datos atribuye a su titular un haz de facultades consistente en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados derechos de hacer [...]».

Así las cosas, la AEPD considera que los juicios de valor sobre la conducta del denunciante realizadas por la DGRN en la resolución de 0000 podrían constituir una intromisión ilegítima en el derecho a la intimidad del denunciante, si bien debieran reconducirse y reclamarse ante la instancia jurisdiccional competente en la materia civil, habida cuenta de que la AEPD carece de competencia para conocer de aquella posible intromisión ilegítima.

#### 4.3. LA PROBLEMÁTICA EN LA PROTECCIÓN DEL DERECHO A LA INTIMIDAD DE LAS PERSONAS JURÍDICAS

Sin duda, uno de los problemas existentes en la normativa vigente es el desamparo en el que se encuentran las personas jurídicas en lo que respecta a la protección de su intimidad.

El derecho a la intimidad se configura como parte de la estructura que conforman

los derechos de la personalidad de las personas físicas, ya que la misma se encuentra anclada al derecho del libre desarrollo de la personalidad. La controversia surge en torno a los entes o personas jurídicas, porque la protección dispensada por la Directiva 95/46/CE al tratamiento de los datos personales contempla únicamente a las personas físicas y, por lo tanto, la trasposición de la normativa europea en nuestro ordenamiento interno en la LOPD así lo ha previsto (me remito a la resolución de la Agencia Española de Protección de Datos de 31 de marzo de 2014 <sup>30</sup>, entre otras).

Por todo lo dicho, las personas jurídicas carecen de los mecanismos de defensa en sede administrativa ante la AEPD y quedan forzadas a un peregrinaje hacia la jurisdicción civil.

#### 4.4. LA GARANTÍA DEL DERECHO A LA INTIMIDAD ANTE LOS ÓRGANOS JUDICIALES

Cuando se trata del derecho a la intimidad y, concretamente, a los datos de carácter personal del ciudadano, tampoco se puede exonerar al poder judicial de su riguroso cumplimiento. La Administración de Justicia debe cumplir con el máximo sigilo el tratamiento de los datos personales del justiciable, al igual que cualquier otro operador jurídico.

Existe abundante normativa jurídica, internacional o nacional, que obliga a la Administración de Justicia en el ejercicio de sus funciones a respetar y proteger la intimidad de las personas: el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea; los artículos 10.1 (la dignidad de la persona) y 18.4 (limitación por ley del uso de la informática como garantía del honor, la intimidad personal y familiar del ciudadano) de la Constitución Española; el título VI de la LOPJ (que recoge los principios y reglas que informan el estatuto y actuación de los jueces y tribunales); o incluso la LOPD, que contempla un catálogo de supuestos exentos de aplicación de la norma (por ejemplo, en materia de terrorismo

o para el Registro Civil), pero nada consta sobre la exención en su aplicación para la Administración de Justicia<sup>31</sup>.

#### 5. LA PROTECCIÓN PENAL DEL DERECHO A LA INTIMIDAD EN EL CÓDIGO PENAL: ESPECIAL REFERENCIA A LAS NUEVAS TECNOLOGÍAS

En este último epígrafe procedo al estudio de la protección jurídico penal de la intimidad. Son de obligado análisis las novedades introducidas por la LO 1/2015, de 30 de marzo, de reforma del Código penal, en vigor desde el 1 de julio de 2015. Esta reforma pretende mejorar la tutela jurídica de la intimidad y castiga conductas en auge como el llamado *revenge porn*. Otra cuestión novedosa ha sido la introducción de un tipo penal cualificado cuando el sujeto activo utilice datos personales de otra persona (una suplantación virtual de la identidad) con la finalidad de vencer la desconfianza de su víctima y lograr vulnerar su esfera íntima. Finalmente, mediante esta reforma de 2015 el legislador continúa adaptando la técnica jurídica de los delitos de intrusismo informático y trata de mejorar la lucha contra estas conductas lesivas e invasoras.

La regulación de los tipos delictivos que protegen el derecho de la intimidad se recoge en el Libro II del CP en el Título X (Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio) que se estructura en dos capítulos: el primero abarca el delito de descubrimiento y revelación de secretos (artículos 197 a 201) y el segundo capítulo engloba las conductas típicas del allanamiento de morada, domicilio de personas jurídicas y establecimientos abiertos al público (artículos 202 a 204). No obstante, mi análisis se centrará en aquellas conductas típicas lesivas del derecho de la intimidad realizadas mediante el uso de las nuevas tecnologías, concretamente

en el artículo 197 en toda su extensión y modalidades.

Este artículo ya había sido reformado por la LO 5/2010, de 22 de junio, que introdujo algunos tipos novedosos como el «intrusismo informático». Como señaló Fernández Teruelo<sup>32</sup>, esta reforma obedecía a la obligación de los Estados miembros de cumplir con la Decisión Marco 2005/222/JAI del Consejo de la Unión Europea de 24 de febrero de 2005, que pretende que los Estados miembros protejan la «seguridad informática» y, en particular, los accesos no consentidos en sistemas informáticos ajenos, pero con medidas penales. El objetivo de la Unión Europea es frenar la creciente actividad delictiva por algunas organizaciones criminales (con clara vocación transfronteriza en sus actividades) y luchar contra actividades terroristas, todo ello dentro de la Red o espacio virtual.

Hay que partir del tipo básico regulado en el artículo 197 CP, que es el pórtico de entrada a las conductas tipificadas en el presente capítulo, el más descriptivo y el más extenso.

El artículo 197.1 CP tiene su *ratio legis* en el antiguo artículo 497 *bis* del CP del 1973, reformado por la LO 18/1994 (TS núm. 1219/2004, 10-12), motivada por los avances de la comunicación general (AP Valencia, sección 4ª, núm. 421/2005, de 2-12). Este primer punto del artículo regula el tipo básico del delito de descubrimiento y revelación de secretos según la doctrina mayoritaria<sup>33</sup>, matizado por otro sector de la comunidad científica que considera que únicamente forma parte del tipo básico el primer inciso del artículo 197.1<sup>34</sup>.

El bien jurídico tutelado es la intimidad; así lo señala el Tribunal Constitucional en la sentencia 134/1999, de fecha 15 de julio, y el Tribunal Supremo, en las sentencias 694/2003, de 20 de junio; núm. 872/2001, de 14 de mayo y núm. 1099/1999, de 24 de junio. Se conculca la intimidad cuando en una actividad personal realizada con otra persona esta dispone de ese hecho o dato, pues la intimidad es un derecho personalísimo que no puede ser compartido

sin el consentimiento de su titular legítimo. Lo que se protege en el derecho fundamental del artículo 18.1 CE, con su proyección penal en el artículo 197 CP, es una dimensión de la intimidad y no el secreto de la misma, como sucede en las comunicaciones<sup>35</sup>. El término «secreto» queda hilvanado a la idea de intimidad, por lo que no debe interpretarse *strictu sensu* en el sentido de «confidencial», sino más bien desde la vertiente de la intimidad o privacidad de las personas. De forma más o menos pacífica, se acepta que el contenido de «secreto» lo constituyen las informaciones o datos que son desconocidos, camuflados o subrepticios para el agente, informaciones que el sujeto pasivo —y titular de la misma— no desea que lleguen a ser conocidas por el sujeto activo<sup>36</sup> y que son solo sabidas por una persona o por un círculo reducido de personas de la confianza del sujeto pasivo.

En numerosas ocasiones surge la fricción entre el derecho a la intimidad y el derecho a la información, conflicto que comporta el análisis de si la conducta es antijurídica o si, por el contrario, tiene encaje en una causa de justificación del artículo 20.7 CP (ejercicio legítimo de un derecho, cargo u oficio). A este respecto, hay que señalar que está fuera de toda duda que las injurias, la rumorología, las insidias o los insultos no tienen la consideración de información, por lo que no quedan amparados por el ejercicio legítimo del derecho a la información<sup>37</sup>.

Nos encontramos ante un delito común en el que el sujeto activo puede ser cualquier persona, pero ha de actuar sin el consentimiento del titular de la intimidad<sup>38</sup>. El sujeto pasivo será el titular del bien jurídico, que coincide con el titular del objeto material del delito<sup>39</sup>. Quedan excluidos de protección como titulares de la intimidad y, por ende, como sujeto pasivo de este delito las Administraciones Públicas, habida cuenta de que el derecho a la intimidad es incompatible con las normas que regulan su actividad —entre otros, los principios de publicidad y transparencia<sup>40</sup>—.

En cuanto a los verbos rectores de la acción del apartado primero del artículo 197, podemos afirmar que este recoge dos tipos básicos con modalidades comisivas distintas.

La primera conducta típica consiste en apoderarse de documentación (papeles, cartas, correos electrónicos, etc.) y la relevancia penal radica en la propia conducta de apropiarse de su contenido sin consentimiento del titular<sup>41</sup>. No es preciso un apoderamiento físico del material; será suficiente para su reproche penal que el agente se haga con la información «íntima» mediante cualquier técnica que permita su reproducción posterior<sup>42</sup>.

La segunda conducta punible es la interceptación de las telecomunicaciones o la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción. Sin duda, el legislador ha querido dejar un *numerus apertus* con la expresión «cualquier otra señal de comunicación». Se trata de una cláusula general dirigida a evitar eventuales lagunas de punición derivadas de los avances tecnológicos. Un sector de la doctrina cataloga la acción típica como de «tipo mixto alternativo»<sup>43</sup>.

En cuanto al elemento del tipo subjetivo, se exige que concurra en el agente una conducta dolosa consistente en el propósito de conocer o descubrir los secretos<sup>44</sup>, o de vulnerar la intimidad de la otra persona sin su consentimiento. En este sentido, y según un sector de la doctrina<sup>45</sup>, el legislador ha introducido la preposición «para» con la clara finalidad de adelantar las barreras punitivas.

La jurisprudencia viene resolviendo que se trata de un tipo delictivo de intención mutilado en dos actos cuya consumación se produce tan pronto como el sujeto activo accede a los datos<sup>46</sup>, sin que se requiera un efectivo descubrimiento del secreto o de la intimidad del sujeto pasivo<sup>47</sup>. De acuerdo con este criterio, la modalidad consistente en la interceptación de las comunicaciones o en la utilización de artificios de grabación se consume cuando tiene lugar dicha interceptación o grabación, con independencia de que el autor llegue o

no al correcto conocimiento de las conversaciones o datos objeto de las mismas<sup>48</sup>. En lo que respecta al *iter criminis*, cabe señalar que encajan formas imperfectas como la tentativa en aquellos casos en que únicamente se ha procedido a la instalación de los sistemas de escucha, grabación o captación de información mediante programas informáticos, sin que se hayan puesto en funcionamiento<sup>49</sup>.

La casuística sobre este tipo delictivo es variopinta: por citar algunos casos reseñables, se ha condenado a un sujeto que fotocopió diversas agendas, expedientes y otros documentos de un abogado<sup>50</sup>; o a un marido que instaló un mecanismo de grabación de conversaciones telefónicas en el domicilio conyugal para comprobar si su esposa le era infiel<sup>51</sup>. Sin embargo la jurisprudencia ha rechazado la condena de aquel que recibe por error diversos correos electrónicos, cuyo contenido no guarda relación alguna con la intimidad de su destinatario<sup>52</sup> o del cónyuge que podía acceder a documentos de carácter profesional y económico en virtud del derecho de información de los cónyuges existente en la sociedad de gananciales<sup>53</sup>; tampoco se condena por un delito contra la intimidad al funcionario de correos que abre las cartas en busca de dinero, cheques o tarjetas de crédito, al realizar la conducta con un exclusivo ánimo de lucro y no de apoderamiento de datos íntimos o personales<sup>54</sup>.

En el art. 197.2 CP el legislador persigue luchar y frenar los abusos informáticos contra la intimidad de las personas. Con este artículo criminaliza conductas que en sede administrativa eran contempladas (y sancionadas) en la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos Personales<sup>55</sup>. Se recogen las conductas penalmente reprochables contra la libertad informática o *habeas data*, también denominado por un sector de la comunidad científica como «delito de abuso informático»<sup>56</sup>. Sin embargo, una corriente doctrinal divergente representada por Bueno Arús y Serrano Gómez<sup>57</sup> critica la utilización de la denominación de «delito informático» y considera que la utilización de

la informática también encaja en otros títulos del Código Penal —por ejemplo, en el ámbito de delitos patrimoniales—.

El bien jurídico protegido es la libertad informática junto a la intimidad de las personas<sup>58</sup>. El sujeto pasivo es el titular de los datos, y en el término «tercero» debe incluirse al sujeto pasivo<sup>59</sup>. El objeto material son aquellos datos reservados de carácter personal registrados en un fichero que el sujeto pasivo (titular de los datos) pretende que no trasciendan fuera de la esfera de la privacidad<sup>60</sup>. El término «reservado» debe entenderse como todo aquello que no es público, a diferencia de «secreto», que es lo desconocido, oculto, aquel reducto más íntimo del sujeto pasivo que el sujeto activo no conoce y que el sujeto pasivo quiere mantener oculto frente a terceros<sup>61</sup>; pero no son los datos más sensibles del núcleo duro de la privacidad, que son objeto del tipo agravado. La conducta típica del agente consiste en apoderarse, acceder, utilizar o modificar datos personales registrados, es decir, usar ilegítimamente los datos personales insertos en un programa informático. Estas conductas requieren de un *animus* específico de causar daño o elemento subjetivo. No obstante, la expresión «en perjuicio de tercero» debe entenderse referida a la invasión de la intimidad y no a la producción de un perjuicio económico o patrimonial concreto<sup>62</sup>. En cuanto al *iter criminis*, la consumación tiene lugar cuando el sujeto activo accede, conoce y tiene a su disposición el dato<sup>63</sup>.

Entre los supuestos de aplicación por nuestros tribunales podemos resaltar el de aquel que se apodera a través de su ordenador de datos personales del padrón municipal<sup>64</sup>; sin embargo, no se considera un dato reservado el número de la cuenta corriente de una persona, pero sí los datos relativos a su saldo, por cuanto revelan la situación económica y la solvencia de su titular<sup>65</sup>.

En el artículo 197.3 CP se castiga la difusión, revelación o cesión a terceros de los datos o información descubierta, así como de las imágenes captadas. El legislador impone en el

primer inciso un tipo agravado; la *ratio legis* es el mayor perjuicio que se produce al revelar, difundir o ceder a terceros los datos reservados y la mayor vulneración de la intimidad a que dan lugar estas conductas<sup>66</sup>. Se trata de un delito compuesto en su modalidad de tipo mixto alternativo, pues exige una de las conductas del artículo 197 en su apartado primero o segundo y, además, difundir, revelar o ceder a terceros los datos o hechos descubiertos o las imágenes captadas. En cuanto al elemento subjetivo, es suficiente la concurrencia de un dolo genérico y no se exige ánimo tendencial específico de causar daño a la intimidad ajena<sup>67</sup>.

En el inciso segundo se castiga al que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realice la conducta descrita en el párrafo anterior. Se trata de un tipo autónomo de revelación de secretos de origen ilícito llamado también «delito de indiscreción»<sup>68</sup>. Tiene su antecedente en el CP 1973 (artículo 497 bis) y supone un límite penal al uso arbitrario o ilegítimo de la libertad de expresión<sup>69</sup>. Requiere como elemento subjetivo del tipo que el agente tenga conocimiento del origen ilícito de los datos o imágenes y, por tanto, del acto previo del que derivan.

Tras la reforma de 2015, en los apartados cuarto, quinto y sexto, del artículo 197 CP han quedado reubicados los tipos agravados y cualificados cuando concurren las siguientes circunstancias:

- que la conducta tipificada en el tipo básico (artículo 197.1 o 2 CP) sea realizada por la persona encargada de los ficheros o de soportes informáticos, o cuando se hayan utilizado datos de la víctima sin su autorización;

- que las conductas típicas del artículo 197 afecten a datos de naturaleza sensible de la persona, *ad exemplum*: ideología, religión, vida o preferencias sexuales, o cuando el sujeto pasivo sea menor de edad o persona incapaz;

- que la conducta del sujeto activo sea realizada con finalidad de lucrarse.

La *ratio legis* de agravar las penas del tipo básico estriba en la especial protección que merece lo que la doctrina denomina el «núcleo duro» del derecho a la intimidad, así como en la necesidad de brindar mayor protección a sujetos especialmente vulnerables como los menores de edad e incapaces<sup>70</sup>. Asimismo, la finalidad lucrativa con la que actúa el agente aumenta el tipo del injusto y, por ende, eleva el reproche penal.

El artículo 197.7 CP ha sido una de las novedades introducidas por la reforma de la LO 1/2015. El legislador penal quiere dar respuesta a la creciente problemática social que se genera cuando, en el contexto de una relación de confianza y de intimidad aceptada se intercambian imágenes o grabaciones, y, una vez quebrada esa relación, una de las partes utiliza esta información para divulgarla a terceros sin el consentimiento de la otra persona. Es lo que en la terminología anglosajona se conoce como el *revenge porn*. Como señala Colás, parece que el legislador ha adaptado la evolución del concepto de intimidad por parte del TC e implementa una suerte de tutela de la facultad positiva del ciudadano de controlar aquello que quiere que sea conocido por terceros de su intimidad<sup>71</sup>.

La conducta rectora es la siguiente: «El que sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona». Es claro, por lo tanto, que estaremos ante imágenes o vídeos «sensibles» que tienen un desarrollo en una esfera muy reducida de intimidad, pero que, expuestos ante la sociedad y fuera del contexto íntimo, acarrearán una lesión a la intimidad de la persona afectada. Con esta nueva figura se pretende evitar anteriores soluciones poco ortodoxas; entre ellas, tratar de darle encaje penal como un delito contra el honor o constreñir a la persona afectada a ejercitar las acciones en la jurisdicción

civil a través de la LO 1/82, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El artículo 197 bis CP recoge las conductas de acceso ilegal a los sistemas informáticos, novedad ya implementada por la LO 5/2010, de 22 de junio, un tipo que trata de luchar contra el «intrusismo informático» y que castiga a los terceros conocidos como *hackers* o *crackers* que, aunque carecen de autorización, sortean los filtros de seguridad y se introducen dentro de sistemas o programas informáticos ajenos, violentando de este modo el «domicilio informático»<sup>72</sup>. La reforma de 2015 modifica la conducta típica y específica en su redacción que tales acciones se proyecten sobre el conjunto o parte del sistema de información. Claramente, la *ratio legis* descansa en el adelantamiento de las barreras punitivas, pues se ha eliminado de la anterior redacción la necesidad de que se acceda efectivamente a los datos o programas. Se mantiene la exigencia de que se vulnere una medida de seguridad, por lo que, *sensu contrario*, la inexistencia de tales medidas conllevaría que la conducta invasora fuera atípica.

En el segundo apartado del citado artículo se introduce una conducta novedosa. Se castigará la interceptación de transmisiones no públicas de datos informáticos. *A priori*, podría confundirse con la conducta del precepto del apartado segundo del artículo 197, pero en este supuesto difiere el bien jurídico, dado que lo que se pretende aquí es proteger la seguridad de los sistemas informáticos y no los secretos o intimidad de otras personas, que quedan protegidos en el artículo 197.1 y 2 CP.

En el artículo 197 ter CP se implanta como novedad la figura de los precursores, y castiga a aquellas personas que faciliten el material necesario (programas informáticos, contraseñas, etc.) a terceros para que puedan llevar a cabo las conductas que atenten contra la intimidad o el *habeas data*.

Los artículos 197 quater y quiquies CP contemplan las figuras agravadas cuando los

sujetos activos actúen en el seno de una organización o grupo criminal, o cuando recaiga la responsabilidad penal sobre una persona jurídica, de conformidad con lo previsto en el artículo 31 bis CP.

El artículo 198 CP regula un tipo cualificado que se justifica por la condición de autoridad o funcionario público del sujeto activo, a quien se le supone el conocimiento del ordenamiento jurídico y que ostenta la representación de máximo garante, por lo que tendrá difícil encaje alegar en sede del elemento de culpabilidad la existencia de un error de prohibición<sup>73</sup>.

En el artículo 199 CP se castiga la acción de divulgar secretos y de incumplir la obligación de sigilo que imponga alguna norma. Con la exigencia de que lo comunicado afecte a la esfera de la intimidad que el titular quiere defender, el artículo plantea la problemática jurídica de discernir la conducta típica de la mera indiscreción del agente. El sujeto activo tiene que ser un profesional que realice una actividad con carácter público y jurídicamente reglamentada<sup>74</sup>.

En el artículo 200 CP se proyecta la protección a los datos reservados de las personas jurídicas cuando estos sean cedidos o revelados sin el correspondiente permiso del representante legal de la persona jurídica.

Finalmente, el artículo 201 CP establece los requisitos de perseguibilidad de las infracciones penales reguladas en el capítulo. Se exige la denuncia previa de la persona agraviada por ser un delito semipúblico (también puede interponerla el representante legal del agraviado —si lo tuviera— o el Ministerio Fiscal si la víctima fuera menor de edad, persona con discapacidad necesitada de especial protección o persona desvalida). No obstante, quedarán exentos del requisito de procedibilidad aquellos supuestos en que el sujeto activo sea un funcionario público o autoridad en el ejercicio de sus funciones —en tal caso, la infracción penal se perseguirá de oficio— o cuando la comisión del delito afectara a los intereses generales o a una pluralidad de personas. Asimis-

mo, el legislador prevé la posibilidad de poner fin al procedimiento mediante la extinción de la acción penal cuando el afectado titular del derecho lesionado otorgue el perdón, con la salvedad de los supuestos regulados en el artículo 130.4 CP, es decir, cuando las víctimas sean menores de edad o incapaces.

## 6. CONCLUSIONES

A la luz de todo lo expuesto, constato el avance de la sociedad en la investigación, la ciencia, la medicina y otros campos, entre los que destaca de manera especial el de las tecnologías de la información y las comunicaciones. Esta evolución vertiginosa puede, en ocasiones, lesionar determinadas parcelas de la vida personal de los ciudadanos. Tal es el caso de los derechos al honor y a la intimidad. A modo de conclusión, cabe apuntar las siguientes notas:

i) En primer lugar, los ciudadanos debemos realizar un ejercicio de autocritica y aceptar que gran parte de la culpa de que la intimidad se encuentre actualmente desprotegida recae sobre nosotros mismos; mantenemos una actitud comprensiva y pasiva y cedemos una cuota de control de nuestra esfera íntima a los poderes públicos bajo el ambiguo y amplio paraguas de la «seguridad nacional»<sup>75</sup>, por citar un solo ejemplo. Asimismo, somos los propios individuos quienes exponemos a diario nuestra intimidad en un «escaparate virtual» con publicaciones de datos personales o fotos de naturaleza familiar e íntima en las diversas plataformas virtuales.

ii) La problemática no parte de la regulación jurídica vigente, sino de la concepción de la esfera íntima característica de la sociedad actual. Recientemente se publicaba un artículo en el periódico *The Guardian*<sup>76</sup> titulado «Privacy is a privilege» donde se aseguraba que disfrutar de una auténtica intimidad se ha convertido en un privilegio.

iii) Hasta la fecha, seguimos ayunos de una regulación legal en sede procesal y nos limitamos a adaptarla como herramienta y Derecho adjetivo a la sociedad contemporánea. Pese a los parches jurídicos introducidos, nuestra decimonónica LECRIM no es capaz de facilitar un elenco de herramientas jurídicas a las fuerzas policiales y los órganos judiciales cuando persiguen conductas delictivas en el ámbito de las TIC.

iv) Finalmente, considero que los poderes públicos deben replantearse su modelo de actuación y proceder a un cambio en sus políticas dirigido a mejorar las garantías de los derechos de sus ciudadanos. Soy consciente de que en el marco de las relaciones internacionales y bajo el prisma de un movimiento global de la población, los Estados están obligados a reforzar sus medidas de seguridad internas. Sin embargo, no es admisible que ante el manido argumento de la «seguridad nacional» se acepte cualquier actuación pública que conlleve

un aniquilamiento del catálogo de derechos fundamentales de sus ciudadanos, como si la etiqueta «seguridad nacional» fuera una patente de corso del siglo XXI. Las polémicas actuaciones de «espionaje masivo» realizadas por muchos Estados son cuando menos «dudosas» (por no decir claramente ilegales) y han sido denunciadas públicamente en numerosos medios (caso Wikileaks<sup>77</sup> o el filtrado de noticias del exagente de la NSA Edward Snowden<sup>78</sup>). Estas intervenciones quebrantan la confianza en las relaciones entre los Estados, pero también la de los ciudadanos que observan el desamparo en el que se encuentra la esfera de su intimidad.

Ya lo afirmaba hace más de cien años con clara vocación de visionario el magistrado del Tribunal Supremo norteamericano Brandeis: «El derecho de que le dejen a uno en paz es el más absoluto de los derechos, y el más valorado por los hombres libres».

## NOTAS

1. «Obama firma la ley que impone límites a la NSA», *El País*, 03/06/ 2015.
2. Herrero-Tejedor, F (1994: 22-23).
3. Warren y Brandeis (1890).
4. Fayos Gardó (2000: 26)
5. Morales Prats (2001).
6. <www.rae.es>.
7. Matallín Evangelio (2013: 386 ss.).
8. Rueda Martín (2004).
9. Cit. *supra*.
10. Rebollo Delgado (2005: 69 ss.).
11. *Ibid.*: 73 ss.
12. <www.listarobinson.es>.
13. Ley 3/2014, de 27 de marzo, por la que se modifica el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios aprobado por Real Decreto Legislativo 1/2007, de 16 de noviembre. Artículo 96 (comunicaciones comerciales a distancia).

14. Giddens (2000).
15. *Ibid.*: 50.
16. *Ibid.*: 171.
17. «Maas warnt vor dem gläsernen Autofahrer», *Die Welt*, 06/07/2014.
18. «Whatsapp, testigo falso», *El País*, 27/06/2014.
19. STS, Sala 2ª, núm. 300/2015, de 19 de mayo (*Tol 5002579*)
20. Bueno Mata (2013).
21. «España busca hackers de los buenos», *El País*, 27/10/2014.
22. Disponible en la página web <[www.agpd.es](http://www.agpd.es)>.
23. Para mayor profundidad, recomiendo la lectura de González Cussac (2011: 267-294).
24. STC núm. 7/2014 de 27 de enero (*Tol 4112436*) o la STC núm. 18/2015, de 16 de febrero (*Tol 4784494*).
25. STC núm. 119/2001 FJ6 o STC núm. 14/2003.
26. STS núm. 425/2014 de 21 de julio de 2014 (*Tol 4526682*).
27. Resolución de la AEPD, R/01226/2014 de 4 de junio de 2014 (*Tol 4363545*).
28. Resolución de la AEPD de 9 de mayo de 2006 (*Tol 955296*).
29. STC núm. 292/2000, de 30 de noviembre.
30. Resolución al recurso núm. TD/00344/2014 de fecha 31 de marzo de 2014 (*Tol 4182267*).
31. Para profundizar en el tema, recomiendo la lectura de Rallo Lombarte (2009).
32. Fernández Teruelo (2011: 195 ss.).
33. Jorge Barreiro, Morales Prats, Paredes Castañón, entre otros (2004: 39).
34. Defienden esta postura Carbonell Mateu o González Cussac (2004).
35. STS núm. 1219/2004, de 10 de diciembre.
36. SAP de Madrid, sección 7ª, núm. 118/2005, de 7 de diciembre.
37. STC núm. 134/1999, de 15 de julio, STC núm. 7/2014 de 27 de enero (*Tol 4112436*).
38. STS núm. 872/2001, de 14 de mayo.
39. STS núm. 694/2003, de 20 de junio; SAP de Gerona, secc. 3ª, núm. 1031/2005, de 14 de noviembre.
40. SAP de Baleares, secc. 2ª, núm. 44/2005, de 19 de mayo.
41. STS núm. 164/2000, de 23 de octubre.
42. STS núm. 1391/2000, de 14-9; SAP de Madrid, secc. 7ª, núm. 118/2005, de 7 de diciembre.
43. Paredes Castañón (2002: 575).
44. STS núm. 872/2001, de 14 de mayo y núm. 446/2001, de 21 de marzo, SAP de Gerona, secc. 3ª, núm. 1031/2005, de 14 de noviembre.
45. Muñoz Conde (2002: 252) y Barreiro (1997: 569).

46. STS núm. 1391/2000, de 14 de septiembre y núm. 234/1999, de 18 de febrero.
47. STS núm. 1219/2004, de 10 de diciembre y núm. 694/2003, de 20 de junio; SAP de Madrid, secc. 7ª, núm. 118/2005, de 7 de diciembre.
48. SAP de Gerona, secc. 3ª, núm. 1031/2005, de 14 de noviembre.
49. STS núm. 694/2003, de 20 de junio y SAP de Gerona, secc. 3ª, núm. 1031/2005, de 14 de noviembre.
50. STS núm. 1391/2000, de 14 de septiembre.
51. STS núm. 872/2001, de 14 de mayo.
52. STS núm. 666/2006, de 19 de julio.
53. AAP de Ciudad Real, 2ª, núm. 92/2006, de 9 de mayo.
54. SAP de Cádiz, secc. 5ª, núm. 10/2006, de 17 de enero.
55. Derogada por la LOPD 15/99, de 13 de diciembre.
56. *Vid.* Jareño Leal y Doval País (1999) o Carbonell Mateu y González Cussac (1996).
57. *Vid.* Bueno Arús (1996) o Serrano Gómez (2003).
58. STS núm. 234/1999, de 18 de febrero.
59. STS núm. 234/1999, de 18 de febrero y STS núm. 1461/2001, de 11 de julio.
60. STS núm. 725/2004, de 11 de junio y núm. 234/1999, de 18 de febrero; SAP de Madrid, secc. 7ª, núm. 118/2005, de 7 de diciembre.
61. STS núm. 234/1999, de 18 de febrero.
62. STS núm. 1461/2001, de 11 de julio; SAP de Castellón, secc. 1ª, núm. 399/2005, de 26 de septiembre.
63. STS núm. 234/1999, de 18 de febrero.
64. STS núm. 1461/2001, de 11 de julio.
65. SAP de Barcelona, secc. 6ª, núm. 219/2006, de 10 de marzo.
66. STS núm. 234/1999, de 18 de febrero; STS núm. 1219/2004, de 10 de diciembre; SAP de Madrid, secc. 7ª, núm. 118/2005, de 7 de diciembre.
67. SAP de Almería, secc. 1ª, núm. 242/2005, de 2 de noviembre.
68. Fernández Teruelo (2011).
69. STS núm. 234/1999, de 18 de febrero; STS núm. 1219/2004, de 10 de diciembre.
70. STS núm. 1219/2004, de 10 de diciembre; SAP de Madrid, 7ª, núm. 118/2005, de 7 de diciembre.
71. Colás Turégano (2015: 667).
72. Fernández Teruelo (2011: 198).
73. STS núm. 367/2001, de 22 de marzo.
74. STS núm. 574/2001, de 4 de abril.
75. Recomiendo la lectura de Cuerda Arnau (2013).
76. «The Great Naked Celebrity Photo leak of 2014 is just the beginning», *The Guardian*, 02/09/ 2014.

77. <http://es.wikipedia.org/wiki/WikiLeaks>: «WikiLeaks (del *inglés* leak, “fuga”, “goteo”, “filtración [de información]”) es una organización mediática internacional *sin ánimo de lucro*, que publica a través de su *sitio web* informes *anónimos* y *documentos filtrados* con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes. El lanzamiento del sitio se realizó en diciembre de 2006, si bien su actividad comenzó en julio de 2007-2008. Desde entonces su base de datos ha crecido constantemente hasta acumular 1,2 millones de documentos. Su creador es *Julian Assange* y está gestionado por *The Sunshine Press*. La organización se ofrece a recibir filtraciones que desvelen comportamientos no éticos ni ortodoxos por parte de los gobiernos, con énfasis especial en los países que considera tienen *regímenes totalitarios*, pero también en asuntos relacionados con religiones y empresas de todo el mundo. De momento, las actuaciones más destacadas de WikiLeaks se han centrado en la *actividad exterior de los Estados Unidos*, especialmente en relación con las guerras de *Irak* y de *Afganistán*».

78. [http://es.wikipedia.org/wiki/Edward\\_Snowden](http://es.wikipedia.org/wiki/Edward_Snowden): «Edward Joseph Snowden (*Elizabeth City, 21 de junio de 1983*) es un consultor tecnológico estadounidense, *informante*, antiguo empleado de la CIA (Agencia Central de Inteligencia) y de la NSA (Agencia de Seguridad Nacional). En junio de 2013, Snowden hizo públicos, a través de los periódicos *The Guardian* y *The Washington Post*, documentos *clasificados como alto secreto* sobre varios programas de la NSA, incluyendo los programas de vigilancia masiva *PRISM* y *XKeyscore*».

## BIBLIOGRAFÍA

- BUENO ARÚS, Francisco (1996): «El delito informático», *Actualidad Informática* núm. 11.
- BUENO MATA, F. (2013): *La prueba electrónica en el marco de una Administración de Justicia informatizada: especial referencia al proceso civil*, Tesis doctoral, USAL.
- BUENO GALLARDO, Esther (2009): *La configuración constitucional del derecho a la intimidad. En particular, el derecho a la intimidad, de los obligados tributarios*, Madrid: Centro de Estudios Políticos y Constitucionales.
- CARBONELL MATEU, Juan Carlos y Jose L. González Cussac (1996): *Comentarios al CP de 1995*, Tomo I, Valencia: Tirant lo Blanch.
- CARRASCO ANDRINO, Mar (2010): «El delito de acceso ilícito a los sistemas informáticos (arts. 197 y 201)», en F. J. Álvarez García y J. L. González Cussac (dirs.), *Comentarios a la Reforma penal de 2010*, Valencia: Tirant lo Blanch, 249-256.
- CARRILLO, Marc (2003): *El derecho a no ser molestado: información y vida privada*, Cizur Menor: Aranzadi.
- CONDE-PUMPIDO FERREIRO, Cándido (2004): *Contestaciones de Derecho penal al programa de judicatura. Parte general*, Madrid: Colex.
- CONTRERAS NAVIDAD, Salvador (2012): *La protección del honor, la intimidad y la propia imagen en Internet*. Thomson Aranzadi.
- COLÁS TURÉGANO, Asunción (2015): «Nuevas conductas delictivas contra la intimidad», en J. L. González Cussac (dir.), *Comentarios a la Reforma del Código Penal de 2015*, Valencia: Tirant lo Blanch.
- CUERDA ARNAU, Marisa (2013): «Intervenciones prospectivas y secreto de las comunicaciones. Cuestiones pendientes», en J. L. González Cussac y Marisa Cuerva Arnau, *Nuevas amenazas a la Seguridad Nacional*, Valencia: Tirant lo Blanch.
- FAYOS GARDÓ, Antonio (2000): *Derecho a la intimidad y medios de comunicación*, Madrid: Centro de Estudios Políticos y Constitucionales.
- FERNÁNDEZ TERUELO, Javier G. (2011): *Derecho penal e internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Valladolid: Lex Nova.
- FRÍGOLS i BRINES, Elisau (2010): «La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías», en J. Boix Reig (dir.) y A. Jareño Leal (coords.), *La protección jurídica de la intimidad*, Madrid: Iustel, 37-90.
- GALÁN MUÑOZ, Alfonso (2006): «Ataques contra sistemas informáticos. Informe sobre la transposición a la normativa penal española de la Decisión-Marco 2005/222/JAI relativa a los ataques contra los sistemas de información», en el Boletín de Información del Ministerio de Justicia, *La armonización del Derecho Penal español: una evaluación legislativa*, año LX suplemento al número 2015.
- (2009): «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales», *Revista Penal*, 24, 90-107.
- (2010): *Libertad de expresión y responsabilidad penal por contenidos ajenos en internet*, Valencia: Tirant lo Blanch.
- (2013): «¿Nuevos riesgos, viejas respuestas?: estudio sobre la protección penal de los datos de carácter personal ante las nuevas tecnologías de la información y la comunicación», *Revista General de Derecho Penal*, 19.

- GARCÍA MEXÍA, Pablo (2014): *Derechos y libertades, Internet y TTCS*, Valencia: Tirant lo Blanch.
- GARCÍA-PABLOS MOLINA, Antonio (1991): «Informática y Derecho Penal», en *Implicaciones sociojurídicas de las tecnologías de la información*, Madrid: Citema.
- GARRIDO FALLA, Fernando (1985): *Comentarios a la Constitución*, Madrid: Civitas.
- GIDDENS, Anthony (2000): *La transformación de la intimidad*, Madrid: Cátedra.
- GONZÁLEZ CUSSAC, Jose L. (2011): «Intromisión en la intimidad y servicios de inteligencia», en F. Muñoz Conde, J. M. Lorenzo Salgado, J. C. Ferré Olivé, E. Cortés Bechiarelli y M. A. Nuñez Paz (coords.), *Un Derecho penal comprometido. Libro homenaje al prof. Dr. Gerardo Landrove Díaz*, Valencia: Tirant lo Blanch, 267-294.
- GONZÁLEZ RUS, Juan José (2006): «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en C. M. Romeo Casabona (coord.), *El Cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada: Comares.
- GREENWALD, Glenn (2014): *Snowden: sin un lugar donde esconderse*, Barcelona: Ediciones B.
- HERRERO TEJEDOR, Fernando (1994): *Honor, intimidad y propia imagen*, Madrid: Colex.
- HUERTA TOCILDO, Susana y Ana C. ANDRÉS DOMÍNGUEZ (2002): «Intimidad e informática», *Revista de Derecho Penal*, núm. 6, 11-71.
- JAREÑO LEAL, Angeles y Antonio DOVAL PAÍS (1999): «Revelación de datos personales, intimidad e informática. Comentario a la STS núm. 234/1998 de 18 de febrero», *La Ley*, 4, 1672-1680.
- JORGE BARREIRO, Agustín (1997): *Comentarios al Código Penal*, Madrid: Civitas.
- LÓPEZ ORTEGA, Juan José (2004): «Intimidad informática y Derecho penal», en *Derecho a la intimidad y nuevas tecnologías, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial*.
- LLOORIA GARCÍA, Paz (2010): «El secreto de las comunicaciones: su interpretación en el ámbito de los delitos cometidos a través de internet. Algunas consideraciones», en J. Boix Reig (dir.) y A. Jareño Leal (coord.), en *La protección jurídica de la intimidad*, Madrid: Iustel.
- MATALLÍN EVANGELIO, Ángela (2013): «El efecto expansivo de los derechos fundamentales a la intimidad y al secreto de las comunicaciones telefónicas», en J. L. González Cussac y M. Cuerda Arnau (dirs.), *Nuevas amenazas a la Seguridad Nacional*, Valencia: Tirant lo Blanch, 379-407.
- MEDINA GUERRERO, Manuel (2005): *La protección constitucional de la intimidad frente a los medios de comunicación*, Valencia: Tirant lo Blanch.
- MENDOZA NAVAS, Natividad (2010): «Los derechos del trabajador», en A. V. Sempere Navarro y P. Charo Baena (dirs.), *Régimen general del contrato de trabajo*, Cizur Menor: Aranzadi.
- MIR PUIG, Carlos (2001): «Sobre algunas cuestiones relevantes del Derecho penal en Internet», *Internet y Derecho penal, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial*, 281-304.
- MORALES PRATS, Fermín (1996): «Protección penal de la intimidad frente al uso ilícito de la informática en el Código Penal de 1995», *Cuadernos de Derecho Judicial, Consejo General del Poder Judicial*, 3, 147-196.
- (2001): «Internet: riesgos para la intimidad», *Cuadernos de Derecho Judicial Internet y Derecho Penal*, 10, 63-82.
- (2015): «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en G. Quintero Olivares (dir.), *Comentarios a la Parte Especial del Derecho Penal*, Pamplona: Thomson-Aranzadi.
- MUÑOZ CONDE, Francisco (2013): *Derecho Penal. Parte especial*, Valencia: Tirant lo Blanch.
- ORTS BERENGUER, Enrique y Jose L. GONZÁLEZ CUSSAC (2011): *Compendio de Derecho penal. Parte general*, Valencia: Tirant lo Blanch.
- ORTS BERENGUER, Enrique y Margarita ROIG TORRES (2005): «Delitos contra la intimidad, utilización fraudulenta de tarjetas de crédito y falsedad en documento electrónico: análisis de casos», en E. Sanjuán (coord.), *Estudios de Derecho Judicial, Consejo General de Poder Judicial. Ejemplar dedicado a la incorporación de las nuevas tecnologías en el comercio: aspectos legales*, 87-128.
- ORTUÑO NAVALÓN, Mari Carmen (2014): *La prueba electrónica ante los tribunales*, Valencia: Tirant lo Blanch.
- PAREDES CASTAÑÓN, José Manuel (2002): *Enciclopedia Jurídica Básica*, Granada: Comares.
- PAYERAS CAPELLA, M. Magdalena y Josep L. FERRER GOMILA (2004): «Explicación técnica de las amenazas de las TIC a la intimidad», en C. Gómez Martínez (dir.), *Cuadernos de Derecho Judicial Derecho a la intimidad y nuevas tecnologías*, 77-106.
- PÉREZ LUÑO, Antonio Enrique (1996): *Manual de Informática y Derecho*, Barcelona: Ariel.
- RALLO LOMBARTE, Artemi (2009): «La garantía del derecho constitucional a la protección de datos personales en los órganos judiciales», en *Nuevas Políticas Públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, Nuevas Políticas Públicas, 97-116.
- (2010): *Derecho y redes sociales*, Madrid: Thomson Reuters.
- REBOLLO DELGADO, Lucrecio (2005): *El derecho fundamental a la intimidad*, Madrid: Dykinson.
- RUEDA MARTÍN, M. Ángeles (2004): *Protección penal de la intimidad personal e informática*, Barcelona: Atelier.

- SERRANO GÓMEZ, Alfonso y Alfonso Serrano Maíllo (2011): *Derecho penal. Parte especial*, Madrid: Dykinson.
- TORRES del MORAL, Antonio (2004): *Principios de Derecho constitucional español*, Madrid: Servicio de Publicaciones Facultad Derecho de la Universidad Complutense de Madrid.
- VIVES ANTÓN, Tomás S., Enrique Orts Berenguer, Juan C. Carbonell Mateu, José L. González Cussac y Carlos Martínez-Buján Pérez (2010): *Derecho Penal. Parte especial*, Valencia: Tirant lo Blanch.
- VIVES ANTÓN, Tomás S. (2013): «El laberinto jurídico español», en J. L. González Cussac y M. Cuerda Arnau (coordinadores), *Nuevas amenazas a la seguridad nacional*, Valencia: Tirant lo Blanch.
- WARREN, Samuel D. y Louis D. BRANDEIS (1890): «The right to privacy», *Harvard Law Review*, 4 (5), 193-220.

**Fecha recepción: 5 de octubre de 2016**  
**Fecha aceptación: 16 de mayo de 2016**