La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español*

Riservatezza, integrità e disponibilità dei sistemi informatici come bene giuridico protetto dai reati informatici nel codice penale spagnolo

Confidentiality, Integrity and Availability of IT Systems as the Interest Protected by the Cyber-Crimes in the Spanish Criminal Code

Dra. Mª Ángeles Rueda Martín
Catedrática de Derecho penal en la Universidad de Zaragoza
marueda@unizar.es

Reati informatici | Delitos informáticos | Cibercrimes

Abstracts

El objeto de la presente investigación reside en estudiar el bien jurídico protegido en los delitos que tipifican determinados ataques contra los sistemas de información en el Código penal español. En concreto, se concluye que la confidencialidad, la integridad y la disponibilidad de los sistemas de información es el bien jurídico protegido. Una vez fundamentada la existencia y la autonomía de dicho bien jurídico se exponen también argumentos que justifican la necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión o peligro del bien jurídico estudiado.

L'obiettivo di questo documento è quello di studiare il bene giuridico protetto dai reati del codice penale spagnolo che puniscono certi attacchi contro i sistemi informatici. In particolare, si conclude che la riservatezza, l'integrità e la disponibilità dei sistemi informatici è l'interesse protetto. Una volta accertata l'esistenza e l'autonomia di questo interesse, vengono avanzate anche argomentazioni per giustificare la necessità politica criminale di tipizzare le condotte che danneggiano o mettono in pericolo il suddetto bene giuridico.

The object of this paper is to study the legal interest protected by the crimes that punish certain attacks against information systems in the Spanish Criminal Code. Specifically, it concludes that the confidentiality, integrity and availability of IT systems is the protected interest. Once the existence and autonomy of this interest has been established, arguments are also put forward to justify the criminal policy need to criminalize conducts that harm or put in danger the said interest.

* Este trabajo se enmarca en el proyecto de investigación "Ciberseguridad y Ciberdelitos" RTI2018-099306-B-100 financiado por el Ministerio de Ciencia, Innovación y Universidades (MCIU), la Agencia Estatal de Investigación (AEI) y el Fondo Europeo de Desarrollo Regional (FEDER), cuyos IPs son los Dres. Carlos Mª Romeo Casabona y Mª Ángeles Rueda Martín. Asimismo desarrolla uno de los objetivos de investigación del Grupo de Estudios Penales de la Universidad de Zaragoza, reconocido como grupo de investigación de referencia por el Departamento de Innovación, Investigación y Universidad del Gobierno de Aragón (BOA 26/03/2020).

Sommario

1. Propuestas de bienes jurídicos protegidos en los delitos contra los sistemas de información. Valoración y consideraciones críticas. – 2. El bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información: fundamentación y autonomía. – 3. Necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos.

1. Propuestas de bienes jurídicos protegidos en los delitos contra los sistemas de información. Valoración y consideraciones críticas.

En este estudio se va a analizar cuál es el bien jurídico protegido en un conjunto de conductas delictivas englobadas en los arts. 197 bis, 197 ter y 264 bis del Código penal español[1], que penalizan una serie de ataques contra los sistemas de información. La integración de este conjunto novedoso de conductas delictivas, por una parte, en los delitos de descubrimiento y revelación de secretos (arts. 197 bis y 197 ter) y, por otra parte, en los delitos de daños (art. 274 bis), nos conduce a preguntarnos en primer término cuál es el bien jurídico protegido, ya que resulta evidente que no tienen como objeto de protección directo la intimidad personal o familiar[2] o el patrimonio, sino los sistemas de información. Una muestra de la evidencia de que la criminalización de los ataques a los sistemas de información no tiene como objeto de protección directo la intimidad personal o familiar, la tenemos en la discusión en torno al bien jurídico protegido en aquellos países que han tipificado en su legislación penal el acceso ilícito a sistemas informáticos. Por ejemplo, en Italia se penaliza en el art. 615 ter del Código penal a quien «acceda sin autorización» a datos y programas informáticos contenidos en todo o en parte de un sistema informático o a quien «se mantenga en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo». Fiandanca y Musco consideran que se protege un interés novedoso, la *privacy* informática, que se sintetiza en la exigencia de que el uso de un sistema informático se produzca en unas condiciones de libertad y autonomía tales que permitan la integridad y la reserva del sistema mismo y de los datos allí recogidos. Estos autores concluyen que el bien jurídico protegido en el mencionado artículo es el denominado "domicilio informático" entendido como la extensión virtual del sujeto titular de un sistema informático[3]. En Alemania la determinación del bien jurídico protegido en el § 202a del Código penal es una cuestión muy controvertida. En dicho precepto se castiga a «quien sin autorización se procura datos, no dirigidos a él y que están particularmente protegidos frente a un acceso indebido, vulnerando las barreras de acceso». Respecto del bien jurídico protegido existen dos propuestas diferenciadas. Por un lado, Möhrenschlager apuntó que lo que se protege es un interés formal en la conservación del secreto de la persona autorizada a disponer sobre el almacenado y transmisión de los datos, que se pone de manifiesto mediante un aseguramiento. Sin embargo, a su

[1] El art. 197 bis establece que «*1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. 2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses*».
El art. 197 ter dispone que «*Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información*».
El art. 264 bis contempla que «*1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero*».

[2] En mi trabajo Rueda Martín (2018), pp. 171 y ss. expongo más extensamente los motivos por los que los delitos tipificados en los arts. 197 bis y 197 ter del Código penal español, no tienen como objeto de protección directo la intimidad personal o familiar.

[3] Véanse Fiandanca y Musco (2006), pp. 244 y 245. En el mismo sentido Caringella *et al.* (2013), pp. 1102 y 1103.

juicio, no es preciso que los datos protegidos constituyan secretos en sentido material, dejando abierta el legislador la cuestión de si se protegen también los intereses del individuo afectado por el contenido de los datos[4]. Por otro lado, Schünemann señala que el bien jurídico protegido en este tipo delictivo es el poder de disposición sobre la información contenida en los datos. En opinión de este autor el § 202a no presupone en particular una lesión del ámbito secreto o vital personal, sino que protege también intereses económicos o de otra clase[5].

En España en relación con el bien jurídico protegido en el delito consistente en un acceso ilícito a sistemas de información, Morón Lerma estima que asistimos a «un nuevo valor social, un interés de nuevo cuño, cifrado en la seguridad de los sistemas informáticos, o en la seguridad informática, o en la seguridad en el funcionamiento de dichos sistemas informáticos». A juicio de esta autora «parece emerger un interés difuso, inmaterial, digno de tutela, pero que, en ningún caso, puede ser identificado, apriorísticamente, con un bien jurídico merecedor de protección penal»[6]. Puente Aba se refiere también al interés relativo a la "seguridad informática", aunque se manifiesta en contra de su configuración como bien jurídico protegido porque no es acorde con los principios de intervención mínima del Derecho penal y con el principio de proporcionalidad[7]. No obstante, otro sector doctrinal considera que la seguridad en los sistemas informáticos sí puede ser considerado el bien jurídico protegido en estos comportamientos, merecedor de protección penal, de carácter supraindividual y difuso[8]. Sin embargo, detrás de esta concepción subyace la necesidad de preservar un determinado ámbito libre de riesgos por la información que alberga, es decir, se exige seguridad en torno al acceso a un sistema informático que contiene información sobre una persona. Desde mi punto de vista, con carácter general, estas definiciones de bienes jurídicos que hacen referencia a la seguridad en relación con el delito que penaliza el acceso no autorizado a sistemas informáticos se caracterizan, de una manera explícita o implícita, por la descripción de una situación de ausencia de riesgos o de lesión para determinados bienes jurídicos que se pueden involucrar en los sistemas de comunicación e información como el patrimonio, la capacidad competitiva de la empresa, la propiedad intelectual, la intimidad personal y familiar, etc. Ahora bien, el valor de la seguridad como bien jurídico no le dota de autonomía, es decir, le impide atribuir a este substrato un valor homogéneo, unitario y autónomo porque no hay una seguridad en sí misma si no es puesta en relación con estos otros bienes jurídicos[9/10].

También se ha concluido que el bien jurídico protegido en estos comportamientos que castigan el acceso ilícito a sistemas de información, es la inviolabilidad del domicilio informático[11]. Por ejemplo, para Morales García el concepto de domicilio informático se centra en el «derecho a mantener los espacios de actuación en red y su contenido al margen de los accesos no deseados, tal como sucede, *ceteris paribus*, con el domicilio "físico"», de modo que el espacio informático lo configura «la información vital que se sitúa en esos espacios que, por tal razón, dada la absoluta miscelánea de elementos privados, públicos, confidenciales, íntimos, reservados, compartibles, etc., determina la reserva del espacio en términos de derecho a la intimidad»[12]. En la sentencia de la Audiencia Provincial de Vizcaya nº. 90307/2004, de 23 julio, se alude también a este bien jurídico "domicilio informático": «el artículo 197.3

[4] Véase Möhrenschlager (1992), p. 137. Véanse también Graf (2017), núm. marginal 2.

[5] Véase Schünemann (2000), núm. marginal 2. En sentido similar Kargl (2017), núm. marginal 3; Hoyer (2016): núm. marginal 1; Lenckner y Eisele (2019), núm. marginal 1.

[6] Véase Morón Lerma (2002), p. 85; Morón Lerma (2007), p. 106.

[7] Véase Puente Aba (2004), pp. 398 y ss.

[8] Véanse Gutiérrez Francés (1991), pp. 619-620; Gutiérrez Francés (1996b), p. 1183; Mir Puig (2002), p. 303; Miró LLinares (2010), marginal nº. 1439; Tomás y Valiente Lanuza (2015), p. 655; Matellanes Rodríguez (2009), p. 68; Anarte Borrallo y Doval País (2016), p. 512; Romeo Casabona (2016), p. 270; Colás Turégano (2015), p. 664. Véase en este sentido la Circular 3/2017 de la Fiscalía General del Estado de España, p. 3, disponible en el enlace https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf.

[9] Como apunta González Rus (2007), p. 21 «tal como aparece concebida y formulada, la seguridad informática no tiene aún, a mi juicio, un contenido sustancial lo suficientemente elaborado y preciso como para permitir una construcción certera de la tutela penal. Prueba de ello es que unas veces se la relaciona con el honor, el patrimonio y la intimidad, y otras, además, con la libertad de información, el secreto de las comunicaciones, la libertad de expresión, etcétera, lo que dice bastante de la ambigüedad del concepto». En este sentido advierten también Anarte Borrallo y Doval País (2016), p. 517 que la seguridad de los sistemas de información «sitúa al intérprete ante un objeto protegido que carece de un sustrato material propio (como siempre ocurre cuando se apela a la *seguridad* de algún objeto)».

[10] Asimismo indica Soto Navarro (2003), p. 236 que las propuestas doctrinales que conceptualizan los bienes jurídicos colectivos en torno a la idea de protección de expectativas de seguridad y confianza, renuncian a la búsqueda de criterios objetivos que permitan fijar el daño social y consideran motivo suficiente para incriminar la aparición de actitudes de preocupación generalizada ante cierto tipo de conductas. A su juicio estas concepciones no garantizan la lesividad verificable en el caso concreto del comportamiento verificado.

[11] Véanse, Alonso de Escamilla (2019), p. 228; Morales García (2010), p. 185.

[12] Véase Morales García (2010), p. 185.

del código penal establece que "el que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años", siendo este delito el denominado de intromisión informática en que lo se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privado de dicha persona». Esta definición del bien jurídico protegido tampoco resulta plenamente convincente, porque limita excesivamente el objeto de protección a la existencia de un espacio "informático" que alberga información vital y, por ello, merecedor de intervención penal. Desde luego que existe este interés en la protección de dicho espacio —que puede encontrar un paralelismo con el bien jurídico "inviolabilidad del domicilio"—, pero no es el único interés que se constata cuando se plantea penalizar conductas que suponen determinados ataques a sistemas de información y comunicación, tal y como se puede deducir de las propuestas político criminales contenidas en el Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001) y en la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de la Unión Europea, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. Por el contrario, hay también un interés en garantizar la confidencialidad e integridad de dichos sistemas por el valor que han adquirido en nuestro desarrollo económico, social y personal, valor que trasciende la necesidad de preservar un simple espacio "informático".

Si nos centramos ahora en el bien jurídico protegido en el delito de obstaculización o interrupción, de una manera grave, del funcionamiento de un sistema de información ajeno del art. 264 bis del Código penal español, aunque la doctrina pone en un primer plano la protección del patrimonio[13], se reconoce que dicha protección no resulta tan clara en los ataques de denegación de servicios en los que existe una sobrecarga de un servidor con múltiples solicitudes que impiden el funcionamiento óptimo del correspondiente sitio web[14], «dada la naturaleza plural de los intereses que se pueden ver afectados por tal comportamiento ilícito en internet. De hecho, su situación como delito patrimonial puede conllevar la no consideración de la dimensión de afectación a la libertad de emisores y receptores en internet de servicios de gran importancia social»[15]. En efecto, los ataques a los sistemas de información y comunicación vulneran o ponen en peligro numerosos intereses que pueden ser individuales o colectivos, plurales y variados. Reducir el bien jurídico protegido en los delitos que criminalizan estos ataques a su dimensión patrimonial, puede conllevar la exclusión de comportamientos que afecten a otros intereses diferentes que deben ser atendidos también, porque configuran unas estructuras y unas relaciones comerciales, administrativas, laborales, formativas, etc., que trascienden el ámbito estrictamente patrimonial y que son radicalmente nuevas[16]. En el delito de Computersabotage del § 303b del StGB, la doctrina alemana estima que el bien jurídico

[13] Comparten esta concepción del bien jurídico del delito tipificado en el art. 264 bis del Código penal Benítez Ortúzar (2016), p. 611; Mestre Delgado (2019), pp. 342 y 343; Muñoz Conde (2019), pp. 433 y 434, quien indica que el delito de daños supone que se disminuya el valor de la cosa dañada, lesionando su esencia o sustancia y añade que la cosa dañada debe tener algún valor patrimonial económicamente valorable. En relación con el delito tipificado en el art. 264 bis del Código penal señala que el concepto de daño incluye la afectación de la posibilidad de uso del objeto material sobre el que recae la acción y conlleva un daño patrimonial; véase el mismo, ob. cit., p. 420.
En Alemania sostiene que el patrimonio es el bien jurídico protegido en el delito de Computersabotage del § 303b del Código penal: Fischer (2020), § 303b, núm. marginal 2. En este precepto se dispone que «*1. El que interfiera de manera relevante en un procesamiento de datos que es de significado esencial para otro, de modo que 1) comete el hecho tipificado en el § 303a; 2) introduce o transmite datos (en el sentido del § 202a 2) con la intención de causar un perjuicio a otro; o 3) destroce, dañe, destruye, inutilice, elimine o modifique un sistema de procesamiento de datos o un soporte de datos, será castigado con una pena privativa de libertad de hasta tres años o con pena de multa. 2. Si el procesamiento de datos es de significado esencial para un negocio o empresa de otros o una administración pública, la pena será privativa de libertad hasta cinco años o pena de multa. 3. La tentativa es punible. 4. En casos particularmente graves del párrafo 2, la pena es privativa de libertad de seis meses a diez años. Un caso particularmente grave suele ser cuando el autor 1) causa un perjuicio de grandes dimensiones, 2) actúa profesionalmente o como miembro de una organización, a la que se ha unido para cometer de manera continuada sabotaje informático, 3) perjudique a través del hecho el suministro de bienes o servicios vitales a la población o la seguridad de la República Federal de Alemania. 5. A los actos preparatorios del hecho punible previsto en el párrafo 1 se aplica consecuentemente el § 202c*».

[14] Véase Renobell Santaren (2019), p. 258.

[15] Véase Miró Llinares (2012), pp. 65 y 66 y Miró Llinares (2016), núm. marginal 4630, quien manifiesta que el legislador debería haber aprovechado la última reforma del CP para integrar los delitos que tienen como referencia "daños informáticos" en un capítulo o sección diferente para «romper definitivamente» las ligaduras interpretativas que acompañan al delito común de daños y que son de difícil encaje en las figuras delictivas de los arts. 264 y 264 bis del CP.

[16] Véanse Lucena Cid (2014), pp. 33 y ss.; Ribagorda Garnacho (1996), p. 310.

protegido es la funcionalidad del procesamiento de datos[17]. Sin embargo, me parece más apropiado destacar los aspectos más esenciales de los sistemas de información, la confidencialidad, la integridad y la disponibilidad, que explican que dichos sistemas ejecuten las diversas funciones que tienen dependiendo del medio concreto (económico, social, administrativo, laboral, sanitario, etc.), en el que se desarrollen y proporcionen su utilidad social.

Precisamente, un importante sector doctrinal ha concluido que los delitos tipificados en los arts. 197 bis, 197 ter y 264 bis CP protegen un nuevo bien jurídico protegido, estrictamente informático, que se lesiona o pone en peligro en todos los delitos que tienen como objeto un sistema de información y de comunicación: la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, de manera que estaremos ante un delito informático cuando se realice una conducta que lesione o ponga en peligro dicho bien jurídico[18]. Por ejemplo, Carrasco Andrino afirma que «se trata de preservar la indemnidad (integridad, confidencialidad, disponibilidad) de los sistemas informáticos como contenedores de información sensible para la intimidad, el honor, el patrimonio, etc. y de los que dependen, además, las infraestructuras y los servicios electrónicos en la nueva Sociedad de la Información»[19]. En una dirección similar se ha pronunciado Morales Prats quien considera que «la protección del Derecho penal se orienta a proteger las redes y sistemas de información, por cuanto la seguridad de los mismos y su capacidad de resistencia, es lo que garantiza la confianza y la certidumbre en la autenticidad e integridad de la información que se contiene en esos sistemas y esas redes. La apuesta es, por tanto, de acuerdo con Carrasco Andrino, por la seguridad en el tráfico informático y por proteger de manera mediata tras la reforma de 2015, la integridad y certeza en los datos y programas informáticos»[20]. De La Mata Barranco plantea también que el bien jurídico protegido en el delito tipificado en el art. 197 bis del Código penal español es la seguridad en el uso de los sistemas de información y comunicación tutelando su confidencialidad y su integridad, por lo que en sí implica para el desarrollo de las relaciones sociales, de modo que ««habrá que esperar que el legislador español aborde globalmente la cuestión del tratamiento de la delincuencia contra datos y sistemas informáticos entendiendo lo que implica la lesividad de estos ataques y habrá que esperar que asuma decididamente un planteamiento en que se atienda la idea de seguridad en el uso de los sistemas de información y comunicación»[21].

Este objeto de protección —la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos— se encuentra expresado en el preámbulo del Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001), donde se pone de relieve la necesidad de «prevenir las acciones que suponen un atentado a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos, así como el uso fraudulento de tales sistemas, redes y datos, velando por la incriminación de aquellos comportamientos descritos en el presente convenio». Asimismo en la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se define en el art. 4 la seguridad de las redes y sistemas de información como «la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos». Además, estudios técnicos sobre seguridad informática recogen también la necesidad de proteger la confidencialidad, la integridad y la disponibilidad

[17] Véanse Möhrenschlager (1986), p. 142; Lackner/Kühl (2018), «§ 303b», núm. marginal 1; Wolf (2008), «§ 303b», núm. marginal 2; Stree/Hecker (2019), «§ 303b», núm. marginal 1; Zaczyk (2017), «§ 303b», núm. marginal 1; Hoyer (2016), núm. marginal 2 y 3 en relación con el § 303b párrafo 2.

[18] Véanse Rodríguez Mourullo *et al.* (2001), p. 260, 261, 262 y 269; Sieber (1998), p. 42, se refiere también a la integridad del sistema informático que resulta vulnerada con las conductas denominadas *hacking*.

[19] Véase Carrasco Andrino (2011), p. 783.

[20] Véase Morales Prats (2016), p. 1478. De forma similar también González Cussac (2016), p. 286; Castelló Nicas (2015), p. 505.

[21] Véase De La Mata Barranco (2016), p. 86. No obstante, continúa este autor «en todo caso, mientras no lo haga y siga atendiendo la tutela de intereses tradicionales (tal como refleja la ubicación del art. 197 bis), lo que sí al menos debe aceptarse es que ya ni importa la intimidad, ni importa el secreto ni importa lo personal. Importa la idea de privacidad informática»; véase el mismo, ob. cit., p. 86. En nuestra jurisprudencia en alguna sentencia se habla de la intimidad informática como bien jurídico protegido, como sucede con la sentencia de la Audiencia Provincial de Madrid sección 2 número 329/2015, de 27 abril, en la que se afirma que: «este nuevo subtipo, sanciona el acceso inconsentido a informaciones ubicadas en el sistema informático (datos, programas ...) o el simple mantenimiento en páginas web ajenas, sin consentimiento del titular, sin necesidad de móvil o acción posterior alguna, y se castiga con pena de hasta dos años. Se castiga, pues, el mero hecho de saltarse las barreras de seguridad informáticas, como un atentado al derecho a la "intimidad informática" pero siempre que exista un acceso a los datos o programas albergados».

de los datos y de los sistemas informáticos[22]. Desde mi punto de vista esta es la línea más adecuada para definir el bien jurídico protegido en la criminalización de determinados ataques contra los sistemas de información, si bien es cierto que es necesario distinguir, por un lado, la confidencialidad, la integridad y la disponibilidad de los sistemas de información y, por otro lado, de los datos propiamente dichos. En el Código penal español ya se protege la obtención, la utilización o modificación de los datos que se almacenen en un sistema informático mediante diversos tipos delictivos en función de la naturaleza de tales datos (arts. 197, 200, 248, 255, 264, 270, 278 o 598), lo que parece sistemáticamente más correcto. Ahora, sin embargo, nos vamos a centrar, exclusivamente en la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, entendiendo por tales, como se indica en el artículo 1 del Convenio del Consejo de Europa sobre Cibercriminalidad «a todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, al ejecutar un programa, el tratamiento automatizado de datos». A continuación, indagaremos tanto en la necesidad de la existencia de este bien jurídico protegido como en su autonomía.

2. El bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información: fundamentación y autonomía.

El Derecho Penal es un sector del ordenamiento jurídico que tiene encomendada la misión de proteger los bienes vitales fundamentales del individuo y la comunidad, los cuales son elevados por la protección de las normas del Derecho a la categoría de bienes jurídicos[23]. Los bienes jurídicos no tienen una entidad material o física, sino que, por el contrario, son valores ideales que se atribuyen por la comunidad social a determinados objetos, cosas, situaciones o relaciones en virtud de su aptitud e idoneidad instrumental para la satisfacción de necesidades individuales y colectivas[24]. Estas necesidades y los intereses que satisfacen ya sean individuales o colectivos son además plurales, variados y, a menudo, también contrapuestos. Sin embargo, el bien jurídico debe ser una entidad libre de conflictos y antagonismos, pues en cuanto instrumento social y políticamente sancionado y dispuesto para la satisfacción de necesidades e intereses plurales[25], el bien jurídico, como afirma Bustos Ramírez, surge como una síntesis normativa (fijada por el ordenamiento jurídico) de una relación social determinada y dinámica[26]. Lo que interesa salvaguardar, entonces, son las relaciones sociales mismas, la posición concreta que en ella ocupan los individuos, su intermediación con objetos y entes, y sus transformaciones por la interacción social. Los bienes jurídicos, concluye Bustos Ramírez, lo que hacen es plasmar de una forma concreta este complejo real social que interesa proteger[27].

Los bienes jurídicos configuran un espacio social que delimita, a su vez, las condiciones necesarias para que otros bienes jurídicos involucrados en dicho espacio, se desenvuelvan correctamente. Cuando estas condiciones necesarias para el desenvolvimiento correcto de los bienes jurídicos se desarrollan con normalidad, posibilitan a los bienes unas mayores posibilidades de rendimiento y aprovechamiento. La normalidad en el desarrollo de estas condiciones necesarias puede, incluso, acarrear la subordinación absoluta de un bien jurídico al cumplimiento de la función social de otro[28]. En este espacio social se puede constatar la existencia de dos clases de bienes jurídicos.

[22] Véanse Ribagorda Garnacho (1996), pp. 307 y ss.; Longstaff *et al.* (1997), pp. 231-255.
[23] Véase Cerezo Mir (2004), p. 13. Véase una reciente exposición de las diversas concepciones del bien jurídico en la actualidad en la obra de Pérez-Sauquillo Muñoz (2019), pp. 40 y ss.
[24] A los efectos que aquí nos interesan acogemos la noción de necesidad de Terradillos Basoco (1981), p. 137 para quien «las necesidades son expresión de valores y cuanto más universales sean éstos, más radicales serán aquéllas. De otro modo no tendría ningún sentido acudir a este criterio que llevaría a un burdo utilitarismo afectado por las mismas limitaciones que las inherentes a la idea de interés. Pero parece atractivo tomar a la necesidad como punto de referencia, pues ello nos permite, de entrada, eliminar los riesgos de postergación del individuo… o de utilización ético-ideológica del Derecho penal… El concepto de necesidad contiene además elementos de generalidad y contrastabilidad que le hacen especialmente apto para ser la base de un discurso racional». Véase. Más adelante concluye que «una política criminal alternativa que pretenda no ser autoritaria ha de limitarse, hoy, a la defensa, de las posibilidades reales de participación igualitaria y ha de tender, por ello, a la satisfacción del máximo de necesidades del máximo número de ciudadanos»; véase *ob. cit*. p. 140.
[25] Véase la noción de necesidad en este contexto desarrollada por Terradillos Basoco (1981), pp. 136 y ss., siguiendo a A. Heller.
[26] Véanse Bustos Ramírez (1987a), p. 138; Bustos Ramírez y Hormazábal Malarée (2006), pp. 71 y ss.
[27] Véase Bustos Ramírez (1987b), p.166.
[28] Véase sobre estas tesis, más ampliamente, Gracia Martín (2006), pp. 224 y ss.

a) Por un lado, existen unos bienes jurídicos de corte clásico cuyas notas más importantes son su fácil determinación, su directa vinculación a la persona en sus relaciones específicas de modo que afectan a las bases mismas de existencia del sistema social, esto es, a las personas y están referidos a las relaciones de una persona con otra, de ahí que sean de tan fácil y elemental delimitación[29]. Estos bienes jurídicos, con carácter general, no admiten quedar involucrados en el quehacer cotidiano de las relaciones sociales y este es el motivo por el que sus afecciones suelen ser de carácter estrictamente personal y puntual[30]. En efecto, la vida, la intimidad personal y familiar o el patrimonio son bienes jurídicos que responden a tales características y que se denominan bienes jurídicos individuales.

b) No obstante, por el dinamismo que ha adquirido la sociedad moderna se han ido configurando unos bienes jurídicos que presentan múltiples dificultades para su determinación y que han recibido la denominación de "bienes jurídicos colectivos"[31]. Una nota característica de estos bienes jurídicos, entre otras[32], es que éstos están ligados al funcionamiento del sistema ya que no se trata sólo de relaciones sociales básicas dentro del sistema y configuradoras del orden social[33]. Ahora bien, estos bienes jurídicos no constituyen una categoría que está por encima del individuo o que va más allá de él, sino que hay «que definirlos a partir de una relación social basada en la satisfacción de necesidades de cada uno de los miembros de la sociedad o de un colectivo y en conformidad con el funcionamiento del sistema social»[34]. Este grupo de bienes jurídicos aparecen como complementarios, desde una perspectiva material, de otros bienes jurídicos que no tienen que ser, exclusivamente, individuales; es decir, tienen que prestar una serie de utilidades a otros bienes jurídicos[35]. La función de los bienes jurídicos colectivos, de prestar utilidades a otros bienes jurídicos, a juicio de Gracia Martín, se bifurca en dos direcciones, de modo que podemos hablar de una doble función según que contemplemos los aspectos de ésta que podemos llamar, respectivamente, negativo y positivo[36]. Por un lado, hay que destacar una función negativa de contención de riesgos para determinados bienes jurídicos reconocida, unánimemente de forma implícita o explícita, en la doctrina lo que explica su relación de complementariedad[37]. Por otro lado, existe asimismo una función positiva de creación y configuración de espacios que delimiten las condiciones en las que los bienes jurídicos a los que complementan pueden cumplir realmente una función social para todos los ciudadanos y que les dota de autonomía[38]. Ambas funciones están estrechamente entrelazadas y sólo por razones expositivas se distinguen. Tampoco debe olvidarse que una vez reconocido por el ordenamiento un bien jurídico colectivo, con carácter general, debe admitirse su independencia y su posibilidad de lesión sin necesidad de exigir un efecto simultáneo sobre bienes jurídicos individuales.

El bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se puedan encontrar involucrados en la función social que desempeñen tales sistemas y redes informáticos, como sucede con la intimidad personal y familiar, el patri-

[29] Véase Bustos Ramírez (1993), pp. 213 y 214.

[30] Véase Bustos Ramírez (1986), p. 158. Naturalmente determinados bienes jurídicos, ya sean estos individuales o colectivos, pueden resultar afectados al encontrarse involucrados de un modo consustancial en una actividad social valorada positivamente por la utilidad general que reporta. Estas afecciones no constituyen un desvalor penal del resultado porque son socialmente adecuadas. Sobre esta tesis, véanse, Rueda Martín (2001), pp. 247 y ss., 251 y ss., 278 y ss.; Gracia Martín (2004), pp. 17 y ss.

[31] Se ha optado por esta denominación bastante utilizada en la doctrina frente a otras denominaciones porque, como indica Soto Navarro (2003), pp. 193 y 194, el adjetivo "colectivo" denota la dualidad de "ser perteneciente o relativo a cualquier agrupación de individuos".

[32] Sobre las características de los bienes jurídicos colectivos, véanse, entre otros, los estudios de Santana Vega (2000), *passim*; Hefendehl (2002), *passim*; Soto Navarro (2003), *passim* y Pérez-Sauquillo Muñoz (2019), *passim*.

[33] Véase Bustos Ramírez (1986), p. 158.

[34] Véase Bustos Ramírez (1986), p. 159.

[35] Véase Bustos Ramírez (1986), p. 159. Este autor, sin embargo, se refiere a la relación de complementariedad entre los bienes jurídicos individuales y los colectivos. De forma similar Santana Vega (2000), p. 91. A mi juicio dicha relación de complementariedad se establece con carácter general entre los bienes jurídicos colectivos y otros bienes jurídicos ya sean individuales o colectivos.
Una consecuencia de esta nota de los bienes jurídicos colectivos es la vertiente positiva del carácter indisponible de dichos bienes jurídicos, contemplada como la posibilidad de aprovechamiento por todos, sin que nadie pueda ser excluido y sin que el aprovechamiento individual obstaculice ni impida el aprovechamiento por otros; véase Hefendehl (2002), pp. 21, 126-128.

[36] Véase Gracia Martín (1994), pp. 210 y 211. En la p. 211, nota 103, pone como ejemplo de bien jurídico colectivo la seguridad e higiene en el trabajo, pues no sólo cumple una función negativa de contención de riesgos para los bienes vida, integridad física y salud, sino la positiva de delimitar un espacio social en que dichos bienes más allá de su existencia material alcancen la calidad adecuada a la dignidad humana.

[37] Véase Bustos Ramírez (1986), pp. 158 y ss.

[38] La doctrina mayoritaria se pronuncia a favor de la autonomía de los bienes jurídicos colectivos. Como ha afirmado Soto Navarro (2003), p. 231 la función social de los bienes jurídicos colectivos permite conceptuarlos de forma autónoma. También aunque de una forma matizada Pérez-Sauquillo Muñoz (2019), pp. 102 y ss.

monio, etc.[39]. Así, por ejemplo, el bien jurídico intimidad personal y familiar puede encontrarse involucrado en la función social que desempeña el bien jurídico relativo a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos. Con respecto al bien jurídico intimidad personal y familiar, el Código penal español organiza un sistema de tipos delictivos recogidos en el artículo 197. En el apartado 2º de este tipo delictivo[40], la protección penal de la intimidad personal y familiar se lleva a cabo a través de unas acciones consistentes, por una parte, en el acceso y la alteración o, por otra parte, en el acceso y la utilización de los datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado por parte de una persona no autorizada, de manera que se realizará la conducta típica del artículo 197.2 del Código penal español siempre y cuando se actúe "en perjuicio del titular de los datos o de un tercero". Estas conductas lesionan el bien jurídico intimidad personal y familiar de una típicamente relevante[41], pero también hay que constatar que con tales comportamientos se produce la lesión de la confidencialidad, integridad y disponibilidad de los sistemas informáticos mediante el simple acceso a los mismos, tanto si se realiza en perjuicio del titular de los datos o de un tercero como si se realiza con la finalidad de descubrir fallos o puertas falsas en dichos sistemas informáticos que albergan archivos de datos reservados. Si se registran unos datos reservados de carácter personal o familiar de una persona en un fichero telemático, la protección del bien jurídico intimidad personal y familiar se reforzará y se asegurará si se protege penalmente la confidencialidad, la integridad y la disponibilidad del sistema que albergue dicho fichero. Lo mismo sucede respecto al bien jurídico relativo a la capacidad competitiva de la empresa, dada la posición ventajosa en las relaciones del tráfico económico que ostenta el titular de la información, entendida como valor económico, protegido en el artículo 278.1 del Código penal español[42], el patrimonio protegido en el artículo 264.1[43] o in-

[39] En relación con el bien jurídico definido como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, Rodríguez Mourullo *et al.* (2001), pp. 261 y 269 apuntan que éste «tiene un carácter instrumental con respecto a otros intereses jurídicamente relevantes, sean éstos objeto directo de protección por el derecho penal o no». Por otra parte, Carrasco Andrino (2011), p. 783 destaca asimismo que el aludido bien jurídico funciona como una barrera de contención de riesgos para otros intereses relevantes (intimidad, patrimonio, seguridad nacional, etc., adquiriendo su protección un carácter instrumental).
La tesis que sostiene que los bienes jurídicos colectivos suponen una barrera de contención de riesgos para bienes jurídicos individuales se encuentra expresada por la doctrina, cuando afirma en relación con determinados delitos que suponen un adelantamiento de las barreras de protección de dichos bienes jurídicos individuales. Por ejemplo, Bolea Bardon (2015), p. 744 indica sobre el bien jurídico protegido en el art. 197 bis que «frente a la tesis que sostiene que el bien jurídico protegido en este delito es la seguridad de los sistemas informáticos, cabe defender que la incriminación de esta conducta supone un adelantamiento de las barreras de protección de la intimidad que parte de la consideración de que la mera intromisión informática pone en peligro la privacidad del titular del sistema». De forma similar Anarte Borrallo y Doval País (2016), p. 513; Queralt Jiménez (2015), p. 313; Miró LLinares (2010), núm. marginal nº. 1438, quien concluye que «la tipificación del *hacking* supone una anticipación de las barreras de protección de la intimidad, puesto que la mera intromisión informática ya pone en *riesgo la privacidad del titular del sistema*… En este sentido, la tipificación del "*hacking*" también supondrá un adelantamiento de las barreras de protección del patrimonio, puesto que con ella se está castigando un acto preparatorio previo para la lesión del bien jurídico». En un sentido parecido Matellanes Rodríguez (2008), p. 66.

[40] En el art. 197.2 se establece que: «*2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán, a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*».

[41] Véase Rueda Martín (2018), p. 118. En este ejemplo, en la medida que se encuentra involucrado el bien jurídico intimidad personal y familiar en estos comportamientos a través de la alteración de los datos reservados contenidos en ese sistema informático, el simple acceso al sistema informático constituirá una tentativa del art. 197.2 del Código penal español, si concurre el elemento subjetivo de lo injusto indicado.

[42] Véase Mayo Calderón (2016), p. 411.
El art. 278.1 del Código penal español establece que «*El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses*». El empleo de alguno de los medios descritos en el art. 197.1 puede suponer el acceso al sistema informático de una empresa que almacene datos o documentos electrónicos que contengan secretos de la misma. Como sucedía con el tipo comentado anteriormente (art. 197.2) si en esta acción no concurre el elemento subjetivo de descubrir un secreto de empresa, quedará impune dicho acceso.

[43] El art. 264.1 del Código penal español establece que «*El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años*». Respecto del bien jurídico protegido en el citado precepto es necesario indicar que hay una discusión doctrinal, ya que entre otras opiniones un sector estima que es el objeto de protección es el patrimonio [véanse, por ejemplo, Mata y Martín (2001), pp. 77 y ss.; González Rus (2005), p. 1471; Navarro Frías (2016), p. 390; Benítez Ortúzar (2016), p. 611; Mestre Delgado (2019), pp. 342 y 343. Muñoz Conde (2019), *Derecho penal, Parte Especial*, 22ª ed., pp. 433 y 434 indica que el delito de daños supone que se disminuya el valor de la cosa dañada, lesionando su esencia o sustancia y añade que la cosa dañada debe tener algún valor patrimonial económicamente valorable. En relación con el delito tipificado en el art. 264 bis del CP señala que el concepto de daño incluye la afectación de la posibilidad de uso del objeto material sobre el que recae la acción y conlleva un daño patrimonial; véase el mismo, ob. cit., p. 420], mientras que otro sector considera que se protege la integridad o disponibilidad de los datos y sistemas informáticos [véanse, por ejemplo, Rodríguez Mourullo *et al.* (2001), pp. 282 y ss.].

cluso la seguridad y/o defensa nacional en relación con el artículo 598 del mismo texto legal[44]. Los mencionados bienes jurídicos se verán más protegidos en tanto en cuanto se garantice la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos en los que se involucren[45]. Este bien jurídico actúa como una barrera de contención de riesgos para otros bienes jurídicos como los citados. Ahora bien, como se ha indicado antes, para que un objeto, situación o relación adquiera la categoría de bien jurídico colectivo es preciso que, además de esa función negativa de contención de riesgos, cumpla una función positiva de creación y configuración de espacios que delimiten las condiciones en que los bienes jurídicos a los que complementan puedan cumplir realmente su función social[46]. Vamos a analizar a continuación si el bien jurídico que estamos estudiando desarrolla esta función positiva.

Si nos detenemos en el funcionamiento del sistema social en la actualidad es innegable la importancia que han adquirido las nuevas tecnologías de la información y de la comunicación (en adelante TIC), con la utilización de redes y sistemas de tratamiento de la información, como medio de crecimiento económico y desarrollo social[47]. Las TIC se han extendido y se han enraizado en nuestras modernas sociedades de tal manera que han conformado unas estructuras y unas relaciones comerciales, administrativas, laborales, formativas, etc., que trascienden el ámbito estrictamente económico y que son radicalmente nuevas[48]. Como se ha señalado anteriormente la generalización de las TIC ha permitido la aparición de nuevos escenarios como, por ejemplo, el comercio electrónico (*e-commerce*), el acercamiento de los bancos a los clientes (*home-banking),* la gestión electrónica de los recursos de las empresas (*e-management*), la gestión doméstica (*domótica*)[49] o la tramitación electrónica entre la ciudadanía y las Administraciones públicas, que sirve mejor a los principios de eficacia y eficiencia y refuerza las garantías de los interesados, como dispone la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas. En el Preámbulo de esta última norma, se dispone que «el desarrollo de las tecnologías de la información y comunicación también ha venido afectando profundamente a la forma y al contenido de las relaciones de la Administración con los ciudadanos y las empresas. Si bien la Ley 30/1992, de 26 de noviembre, ya fue consciente del impacto de las nuevas tecnologías en las relaciones administrativas, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, les otorgó carta de naturaleza legal, al establecer el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y sistemas necesarios para que ese derecho pudiera ejercerse. Sin embargo, en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos, sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados». En estos escenarios enmarcados en la utilización de las TIC se involucran bienes jurídicos tales como el patrimonio, la intimidad personal y familiar o la capacidad competitiva de la empresa, de manera que los sistemas de información y comunicación permiten su desarrollo en las modernas sociedades.

Nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de unos sistemas y redes de información, por lo que de los

[44] El art. 598 del Código penal español establece que «*El que, sin propósito de favorecer a una potencia extranjera, se procurare, revelare, falseare o inutilizare información legalmente calificada como reservada o secreta, relacionada con la seguridad nacional o la defensa nacional o relativa a los medios técnicos o sistemas empleados por las Fuerzas Armadas o las industrias de interés militar, será castigado con las penas de prisión de uno a cuatro años*». En relación con el bien jurídico defensa nacional, véase, De Miguel Beriain (2016), p. 848.

[45] Véase Miró LLinares (2010), número marginal nº. 1438.

[46] Véase Gracia Martín (1994), pp. 210-211.

[47] Véanse Romeo Casabona (1988), pp. 19 y ss.; Gutiérrez Francés (1996a), pp. 250 y 274. Al comienzo de la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE de 23 de junio de 2007), se indica que «las tecnologías de la información y las comunicaciones están afectando también muy profundamente a la forma e incluso al contenido de las relaciones de los seres humanos entre sí y de las sociedades en que se integran».

[48] Véanse Lucena Cid (2014): pp. 33 y ss.; Ribagorda Garnacho (1996), p. 310. Estas estructuras y relaciones se pueden mantener mediante el ordenador e internet, pero también mediante SMS o la Televisión Digital. En cualquier caso en un futuro más o menos inmediato pueden aparecer otros canales que aún no están disponibles hoy en día.

[49] Véase Salom Clotet (2006), pp. 93 y ss.

riesgos que se derivan de su vulnerabilidad[50] ha surgido, consecuentemente, un interés en la seguridad de la utilización de las TIC, que ha sido refrendado claramente en el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, y en el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Cuando el Derecho protege las TIC, reconoce su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. La necesidad de proteger los sistemas de comunicación e información por dicho valor social se ha reconocido también, por ejemplo, en la sentencia del Tribunal Constitucional alemán de 27 de febrero de 2008 que establece en su parágrafo nº. 181 que: «c) De la importancia de la utilización de los sistemas tecnológicos de información para el desarrollo de la personalidad y de los peligros para la misma unidos a dicha utilización, resulta una importante necesidad de protección desde el punto de vista de los derechos fundamentales. Los particulares exigen que el Estado atienda las expectativas de confidencialidad e integridad de tales sistemas justificadas en el marco del libre desarrollo de la personalidad»[51]. Y, posteriormente, en el parágrafo 203 afirma que: «Por otra parte, el derecho fundamental a la garantía de la integridad y confidencialidad de los sistemas tecnológicos de información hay que esgrimirlo cuando la facultad de injerencia afecte a un sistema, que por sí solo o en conexión con redes tecnológicas, en un contorno cerrado o amplio, pueda contener datos del afectado referentes a su persona, de modo que el acceso al sistema permitiría formarse una idea sobre aspectos esenciales de la vida de una persona o incluso obtener una imagen representativa de su personalidad»[52].

La utilización de las TIC en los ámbitos reseñados ha conducido al surgimiento de unos intereses que tienen unas notas comunes[53]. Por una parte, los particulares tienen interés en que se proteja la integridad o la confidencialidad de los sistemas informáticos al margen de los contenidos de naturaleza personal o patrimonial que se almacenen en los mismos[54], como un instrumento que facilita sus relaciones sociales, económicas, etc. También las empresas tienen en los modernos sistemas informáticos un instrumento que facilita y potencia su actividad económica y que supone una notable ventaja competitiva en el mercado[55], y tienen interés en que se proteja no sólo el contenido de la información que almacenan, sino además la confidencialidad y la integridad de dicho sistema. Del mismo modo, los organismos públicos tienen interés en la protección de los sistemas informáticos que almacenan los datos personales de todo tipo o que regulan las relaciones de las distintas administraciones con los administrados, fundamental para el debido funcionamiento de las mismas. Además de este interés generalizado debemos observar que la realización de diversas operaciones económicas, financieras, empresariales, laborales, administrativas, etc. por parte de los usuarios tiene que llevarse a cabo de una forma práctica pero segura, es decir, garantizando tanto la disponibilidad del sistema informático como la identidad o la autenticación de la persona que accede a dicho sistema. Los usuarios (administrados, empresas, etc.) tienen interés en que cumpliendo unos determinados requisitos se pueda acceder a dichos sistemas informáticos para llevar a cabo aquellas operaciones que sean relevantes, sin que se interpongan demasiados obstáculos. En suma nos

[50] Rodríguez Mourullo *et al.* (2001), p. 257 señalan asimismo que «los estudios doctrinales y los informes de agencias internacionales y de organizaciones públicas y privadas han advertido una y otra vez sobre los riesgos derivados de la vulnerabilidad de unos sistemas y redes informáticos de los que toda la organización social (el sistema financiero, las infraestructuras básicas, las empresas, los organismos públicos, los particulares) ha pasado a depender de forma extraordinaria».

[51] Véase BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 - Rn. (1-333), disponible en la dirección http://www.bverfg.de/e/rs20080227_1bvr037007.html. La redacción original del parágrafo traducido es la siguiente: «c) Aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind, folgt ein grundrechtlich erhebliches Schutzbedürfnis. Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet».

[52] La redacción original del parágrafo traducido es la siguiente: «Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist hingegen anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten».

[53] En la STC alemán de 27 de febrero de 2008 —BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 -1 BvR 370/07- Rn. (1-333)— en su parágrafo 204 disponible en la dirección http://www.bverfg.de/e/rs20080227_1bvr037007.html, se reconoce también con carácter general el interés de los interesados que utilizan sistemas tecnológicos de información en garantizar la confidencialidad e integridad de dichos sistemas.

[54] Véanse Gutiérrez Francés (1996a), p. 301; Matellanes Rodríguez (2008), p. 65.

[55] Véase Gutiérrez Francés (1996a), p. 274, quien destaca que la informatización para las empresas implica contabilidades, carteras de clientes, balances, informes y proyectos empresariales, estrategias de mercado, procedimientos económicos o tecnológicos de carácter reservado, o datos de investigación y desarrollo de tecnología.

encontramos con la convergencia de todos estos intereses que explican, por una parte, la función social de los sistemas de información y comunicación como importantes herramientas de crecimiento y desarrollo económico y social; y, por otra parte, explican la demanda de medidas de seguridad de carácter técnico y de organización en su utilización, que incluyen mecanismos y prácticas profesionales que permiten tanto un uso continuado de las tecnologías como el establecimiento de acciones destinadas a interrumpir o sabotear su funcionamiento o la interpretación de datos elaborados y tratados por otros[56].

Esta seguridad en la utilización de los sistemas informáticos de forma más o menos generalizada se manifiesta en la confidencialidad, integridad y la disponibilidad de los sistemas de comunicación e información[57], y que constituye propiamente el bien jurídico a proteger en la criminalización de determinados ataques contra los sistemas de información. La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s. La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s. La disponibilidad hace referencia al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s. De esta manera, por ejemplo, cuando un *hacker* penetra ilícitamente en un sistema informático ajeno, tanto si se han infringido medidas de carácter técnico como si no ha sido así, se encuentra en un espacio, el propio sistema, en el que su integridad se ha visto afectada porque la sola entrada y el consiguiente uso del sistema da lugar a modificaciones en los datos del mismo, junto con las alteraciones de tales datos para intentar borrar los rastros que pudieran identificarles. Asimismo, la confidencialidad del sistema se ve afectada si se utiliza por parte de una persona que no está autorizada. Finalmente, la disponibilidad del sistema se afecta cuando penetra una persona no autorizada. Se puede constatar que en estos supuestos de accesos ilícitos a un sistema informático se vulnera el bien jurídico expuesto con independencia de las ulteriores finalidades que haya perseguido el *hacker* con tales entradas.

Se suele afirmar, con carácter general, que estas conductas de *hacking* blanco son más beneficiosas que perjudiciales ya que revelan las deficiencias de los sistemas informáticos a los encargados de la seguridad de los mismos, a quienes también se favorece con la posterior comunicación de tales deficiencias con el fin de fortalecer la seguridad de los mencionados sistemas. Al respecto cabe señalar, en primer lugar, que este argumento sólo es atendible si el *hacker*, una vez descubierta la vulnerabilidad de un sistema y producido el acceso, informa directamente a los administradores o a los encargados de la seguridad de los sistemas. El problema se centra más bien en que cuando se descubre una vulnerabilidad en un sistema aparece el denominado "*exploit*", que en el entorno *hacker* se refiere al método concreto de explotar una vulnerabilidad. Normalmente un "*exploit*" se presenta como un programa, que puede estar creado en cualquier lenguaje, y que aprovecha algún error del sistema operativo, por ejemplo, para obtener los privilegios del administrador y así tener un control total del sistema[58]. Estos "*exploits*" se publican en webs especializadas por lo que se difunden las vulnerabilidades descubiertas a través de diversas vías como los canales IRC (Internet Relay Chat) que los *hackers* establecen para dar a conocer sus accesos y sus operaciones, pero antes de publicarse se ofrece un tiempo a los administradores de los sistemas para que solucionen las vulnerabilidades descubiertas. La licitud de esta forma de proceder podría aceptarse si partimos de la consideración de que estos comportamientos de *hacking* blanco comportan una utilidad social general, y ello será así cuando la finalidad sea revelar las deficiencias de los sistemas informáticos a los encargados de la seguridad de los mismos, a quienes también se favorece con la posterior comunicación de tales deficiencias con el fin de fortalecer la seguridad de los mencionados sistemas. Numerosas empresas de productos de seguridad disponen de bases de datos actualizadas con las vulnerabilidades, su descripción técnica y su solución y los fabricantes de programas tienen que actualizar sus productos constantemente para evitar las vulnerabilidades que se van descubriendo[59] ya sea por sí mismos o por la comunicación de algún *hacker*. Sin embargo, no puede valorarse como socialmente útil aquel comportamiento de *hacking* en el que se haya descubierto la

[56] Sobre esta demanda de medidas de seguridad de carácter técnico y de organización, véase Morón Lerma (2002), p. 48. En cuanto a las medidas de seguridad, desde un punto de vista técnico, véase la exposición realizada por Huidobro Moya *et al.* (2005), *passim*; Ribagorda Garnacho (2008), pp. 381 y ss.
[57] Véase Ribagorda Garnacho (1996), pp. 312 y 313.
[58] Véase Piqueres Castellote (2006), p. 62.
[59] Véase Piqueres Castellote (2006), p. 62.

vulnerabilidad de un sistema, y una vez producido el acceso no se informe de ningún modo a los administradores o a los encargados de la seguridad de los sistemas. En segundo lugar, este mismo fin de encontrar fallos en los sistemas informáticos y de fortalecer, así, la seguridad de los sistemas informáticos, se consigue con la disposición de las necesarias medidas de seguridad de carácter técnico y de organización por parte de las empresas competentes, por lo que la función que un *hacker* ajeno al sistema realice se desempeñaría igualmente por personal adecuado y con garantías. En ocasiones se argumenta también que el *hacking* suele ser una actividad de estudio o de investigación y que por este motivo resulta exagerado criminalizar a aquellos *hackers* que persiguen únicamente aprender. Si se realizan estas actividades de estudio y de investigación puede solicitarse una autorización al administrador o encargado del sistema informático, por lo que ya no sería un acceso ilícito siempre y cuando se cumplieran todos los requisitos para los que se otorga dicha autorización.

Del desarrollo de la función positiva del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos se derivan algunas consecuencias que exponemos a continuación. En primer lugar, se justifica que no sea necesario añadir ninguna finalidad ilícita adicional a las conductas de *hacking* para que intervenga el Derecho penal, porque para constatar una perturbación en la función social del bien jurídico indicado no es necesario que concurra una finalidad específica adicional referida a la involucración de otros bienes jurídicos en el contexto en el que aquél desarrolle su función positiva. La existencia de una finalidad adicional nos ayudará sólo a delimitar los comportamientos ilícitos que se centran en la "información" almacenada, tratada y transmitida mediante un sistema informático[60], pero a mi juicio no es necesaria para delimitar las acciones que lesionen o pongan en peligro el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Este bien merece la protección del ordenamiento jurídico y dada la importante función social que desempeña, se legitima la intervención del Derecho penal en su protección, así como en la represión de aquellos comportamientos que lo lesionen[61]. En segundo lugar, la incorporación de ulteriores exigencias objetivas para incriminar las conductas de *hacking*, como la vulneración de las medidas de seguridad del sistema, puede ser admitida desde un punto de vista político criminal como manifestación de una mayor gravedad de tales comportamientos.

3. Necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos.

Una vez fundamentada la existencia y la autonomía del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, debemos exponer argumentos que justifiquen la necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión del bien jurídico estudiado. En primer lugar, cabe destacar la importancia de proteger penalmente y no sólo administrativamente la función social que desempeña el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Ya hemos explicado que nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de la utilización de unos sistemas y redes informáticos, como medio de crecimiento económico y desarrollo social. En los últimos años el Derecho ha desplegado una regulación y protección de las nuevas tecnologías de la información y comunicación, y ha reconocido su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. Consecuentemente ha surgido también un interés en la seguridad de la utilización de las TIC desde diversos ámbitos, que se

[60] Véase Gutiérrez Francés (1996a), pp. 274 y 275.

[61] Con la exposición que ha precedido a estas conclusiones se ha intentado responder a una pregunta central que ha planteado claramente González Rus (2007), p. 31: «si la informática e internet suponen factores de peligro adicional para los derechos e intereses individuales y sociales que no estén cubiertos (y que no puedan ser cubiertos) con la aplicación (y, eventualmente, con la complementación y ampliación) de las figuras delictivas actualmente disponibles dirigidas a la protección de bienes jurídicos personales, colectivos y generales. Sólo a partir de ahí podrá determinarse si es necesaria para la tutela de los bienes e intereses implicados en las redes de transmisión de datos e internet la creación de "nuevos" bienes jurídicos específicos de naturaleza informática».

concreta en la confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido dotado de autonomía y que, además, sirve de barrera de contención de riesgos para otros bienes jurídicos que puedan verse implicados en la utilización de sistemas y redes informáticos. En segundo lugar, elevar a la categoría de delito en el Código penal español esta clase comportamientos que supongan un ataque contra los sistemas de comunicación o información, supone una obligada armonización penal en este ámbito de nuestra legislación con lo dispuesto en otros estados de la Unión Europea, en consonancia con lo establecido en el Reglamento (UE) 2019/796 del Consejo de la Unión Europea, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, en la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de la Unión Europea, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que derogó la Decisión Marco 2005/222/JAI, y en el Convenio del Consejo de Europa sobre Ciberciminalidad de 23 de noviembre de 2001. Dicha armonización es necesaria además porque en esta clase de ataques podemos encontrar una nota que le añade un especial grado de peligrosidad: su conexión internacional o transfronteriza, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto, y resulta sorprendente que en algún territorio un acceso ilegal a sistemas informáticos con independencia de la finalidad que haya tenido quien accede, resulte impune[62]. En tercer lugar, hay que tener en cuenta que, como afirma Romeo Casabona, el ciberespacio presenta unos perfiles de gran interés para el Derecho penal entre los que destaca la potencialidad multiplicadora de las acciones ilícitas y de sus efectos lesivos para los bienes jurídicos afectados[63]. Esta característica se puede apreciar con especial intensidad en las conductas de acceso ilícito a sistemas informáticos, que como ha puesto de relieve un sector doctrinal tienen un efecto criminógeno[64]. Por ello y con carácter general, el ciberespacio se presenta en las sociedades modernas como una de las posibles fuentes de riesgos necesitados de control, y dada la gravedad de sus repercusiones sobre diferentes bienes jurídicos se legitima la intervención del Derecho penal.

Bibliografía

Alonso de Escamilla, Avelina (2019): "Tema 10. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en Lamarca Pérez, Carmen (coordinadora): *Delitos. La parte especial del Derecho penal,* 3ª ed., (Madrid, Colex), pp. 227-248.

Anarte Borrallo, Enrique, Doval País, Antonio (2016): "Lección 19. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio (1). Delitos de descubrimiento y revelación de secretos", en Boix Reig, Francisco Javier (director): *Derecho penal, Parte Especial, Volumen I, La protección penal de los intereses jurídicos personales. (Adaptado a la reforma de 2015 del Código penal)*, 2ª ed., (Madrid, Iustel), pp. 493-549.

Benítez Ortúzar (2016): "Capítulo 26. Delitos contra el patrimonio y el orden socioeconómico (VIII). De la alteración de precios en concurso y subastas públicas. De los daños. Disposiciones comunes a los delitos patrimoniales", en Morillas Cueva, Lorenzo (director): *Sistema de Derecho penal, Parte Especial,* 2ª ed., (Madrid, Dykinson), pp. 693-621.

Bolea Bardon, Carolina (2015): "Artículo 197 bis", en Corcoy Bidasolo, Mirentxu y Mir Puig, Santiago (directores), Vera Sánchez, Juan Sebastián (coordinador): *Comentarios al Código penal. Reforma LO 1/2015 y LO 2/2015*, (Valencia, Tirant lo blanch), pp. 744-746.

Bustos Ramírez, Juan José (1987a): "Del estado actual de la teoría del injusto", en *Control social y sistema penal*, (Barcelona, PPU), pp. 125-140.

[62] Véase sobre esta necesidad De La Mata Barranco (2015), pp. 71 y ss.
[63] Véase Romeo Casabona (2006), p. 4. También destacan, con carácter general, el factor criminógeno del procesamiento electrónico de datos, Sieber (1977), pp. 158 y ss.; Mata y Martín (2001): pp. 17, 24 y ss.; Morón Lerma (2002), p. 75.
[64] Véase respecto de las conductas de hacking, Gutiérrez Francés (1996b), pp. 1179 y ss.; Gutiérrez Francés (1994), p. 206.

Bustos Ramírez, Juan José (1986): "Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)", *Revista de la Facultad de Derecho de la Universidad Complutense*, *Estudios de derecho Penal en homenaje a Luis Jiménez de Asua*, número extraordinario 11, pp. 147-164.

Bustos Ramírez, Juan José (1993): "Perspectivas actuales del Derecho Penal Económico", en *Política criminal y reforma penal. Homenaje a la memoria del Profesor Dr. D. Juan del Rosal*, Editorial Revista de Derecho privado, (Madrid, Editoriales de Derecho Reunidas), pp. 213-224.

Bustos Ramírez, Juan José (1987b): "Política criminal e injusto. (Política criminal, bien jurídico, desvalor de acto y de resultado)", en *Control social y sistema penal*, (Barcelona, PPU), pp. 159-180.

Bustos Ramírez, Juan José y Hormazábal Malarée, Hernán (2006): *Lecciones de Derecho penal, Parte General,* (Madrid, Editorial Trotta).

Caringella, Francesco, De Palma, Michele, Farini, Sara, Trinci, Alessandro (2013): *Manuale di Diritto penale, Parte speciale,* 3ª ed., (Roma, Dike Giuridica Editrice).

Carrasco Andrino, María del Mar (2011): "Lección 23ª. Descubrimiento y revelación de secretos", en Álvarez García, Francisco Javier (director), Manjón-Cabeza, Araceli y Ventura Püschel, Arturo (coordinadores): *Derecho penal español, Parte Especial (I),* 2ª ed., (Valencia, Tirant lo blanch), pp. 753-806.

Castelló Nicas, Nuria (2015): "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor", en Morillas Cuevas, Lorenzo (director): *Estudios sobre el Código penal reformado. (Leyes Orgánicas 1/2015 y 2/2015)*, (Madrid, Dykinson), pp. 487-514.

Cerezo Mir, José (2004): *Curso de Derecho penal español, Parte General, I. Introducción*, 6ª ed., (Madrid, Tecnos).

Colás Turégano, María Asunción (2015): "Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)", en González Cussac, José Luis (director), Matallín Evangelio, Ángela y Górriz Royo, Elena (coordinadoras): *Comentarios a la reforma del Código penal de 2015*, (Valencia, Tirant lo blanch), pp. 663-684.

De La Mata Barranco, Norberto (2016): "Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis CP). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación", *Cuadernos de política criminal*, n.º 118, pp. 43-86.

De La Mata Barranco, Norberto (2015): *Derecho penal europeo y legislación española: las reformas del Código penal. Actualizado a la reforma penal 2015*, (Valencia, Tirant lo blanch).

De Miguel Beriain, Íñigo (2016): "Capítulo 36. Delitos de traición y contra la paz o la independencia del estado, y relativos a la defensa nacional", en Romeo Casabona, Carlos, Sola Reche, Esteban, Boldova Pasamar, Miguel Ángel (coordinadores): *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, (Granada, Comares), pp. 837-851.

Fiandanca, Giovanni y Musco Enzo (2006): *Diritto penale, Parte speciale, Volume II, tomo primo, I delitti contro la persona*, 1ª ed., (Bologna, Zanichelli editore).

Fischer, Thomas (2020), "§ 303b", *Strafgesetzbuch mit Nebengesetzen Kommentar*, 67 Auflage, (München, C. H. Beck).

González Cussac, José Luis (2016): "Lección XV. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en González Cussac, José Luis (coordinador): *Derecho penal, Parte Especial,* 5ª ed. actualizada a la Ley Orgánica 1/2015, (Va-

lencia, Tirant lo blanch), pp. 273-297.

González Rus, Juan José (2005): "Daños a través de internet y denegación de servicios", en Jorge Barreiro, Agustín (coordinador): *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo*, (Madrid, Civitas), pp. 1469-1488.

González Rus, Juan José (2007): "Precisiones conceptuales y político-criminales sobre la intervención penal en Internet", *Delito e informática: algunos aspectos*, *Cuadernos penales José María Lidón*, número 4, (Bilbao, Universidad de Deusto), pp. 13-40.

Gracia Martín, Luis (2004): "El finalismo como método sintético real-normativo para la construcción de la teoría del delito", *Revista Electrónica de Ciencia Penal y Criminología* 06-07, pp. 1-22.

Gracia Martín, Luis (1994): "Nuevas perspectivas del Derecho penal tributario. (Las funciones del tributo como bien jurídico)", *Actualidad Penal*, número 10, pp. 183-217.

Gracia Martín, Luis (2006): *Fundamentos de dogmática penal. Una introducción a la concepción finalista de la responsabilidad penal*, (Barcelona, Atelier).

Graf, Jürgen Peter (2017): «§202a», en Joecks, Wolfgang y Miebach, Klaus (coordinadores), *Münchener Kommentar, Strafgesetzbuch*, Band 4 §§ 185-262 StGB, 3ª Auf., (München, C. H. Beck).

Gutiérrez Francés, María Luz (1996a): "Delincuencia económica e informática en el nuevo Código penal", en Gallardo Ortiz, Miguel Ángel (director) : *Ámbito jurídico de las tecnologías de la información*, *Cuadernos de Derecho Judicial*, (Madrid, Consejo General del Poder Judicial), pp. 247-306.

Gutiérrez Francés, María Luz (1996b): "El intrusismo informático (Hacking): ¿Represión penal autónoma?", *Informática y derecho: Revista iberoamericana de derecho informático*, (Ejemplar dedicado a: II Congreso Internacional de Informática y Derecho. Actas (volumen II), pp. 1163-1184.

Gutiérrez Francés, María Luz (1991): *Fraude informático y estafa,* (Madrid, Ministerio de Justicia, Centro de Publicaciones).

Gutiérrez Francés, María Luz (1994): "Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa", en Tiedemann, Klaus y Arroyo Zapatero, Luis Alberto (editores): *Estudios de Derecho penal económico*, (Cuenca, Ediciones de la Universidad de Castilla-La Mancha), pp. 183-208.

Hefendehl, Roland (2002): *Grund un Grenzen des Schutzes kollektiver Rechtsgüter im Strafrecht*, (Köln, Carl Heymanns Verlag KG).

Hoyer, Andreas (2016): "Kommentar zur § 303b", en Wolter, Jürgen (editor): *SK-StGB, Systematischer Kommentar zum Strafgesetzbuch*, 9ª Auf., (Köln, Carl Heymanns), pp. 17-27.

Huidobro Moya, José Manuel y Roldán Martínez, David (2005): *Seguridad en redes y sistemas informáticos,* (Madrid, Thomson Paraninfo).

Kargl, Walter (2017): "Kommentar zur §202a StGB", en Kindhäuser, Urs, Neumann, Ulfrid y Paeffgen, Hans-Ullrich (editores): *Nomos Kommentar, Strafgesetzbuch*, Band 2, 5 Auf., (Baden-Baden, Nomos Verlagsgesellschaft), pp. 1577-1594.

Lackner, Karl y Kühl, Kristian (2018), "§ 303b", *Strafgesetzbuch Kommentar*, 29 Auflage, (München, C. H. Beck).

Lenckner, Theodor y Eisele, Jörg (2019): "Kommentar zur § 202a", en Schönke, Adolf, Schröder, Horst, Eser, Albin *et alium* (autores): *Strafgesetzbuch Kommentar*, 30 Auf., (München, C. H. Beck).

Longstaff, Thomas, Ellis, James, Hernan, Shawn, Lipson, Howard, McMillan, Robert, Pesante, Linda y Simmel, Derek (1997): "Security of the Internet", en Froehlich, Fritz y Kent, Allen (eds.), *The Froehlich/Kent Encyclopedia of Telecommunications*, vol. 15, (New York, Marcel Dekker, Inc.).

Lucena Cid, Isabel Victoria (2014): "El concepto de la intimidad en los nuevos contextos tecnológicos", en Galán Muñoz, Alfonso y Arribas León, Mónica (coordinadores.): *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*, (Valencia, Tirant lo blanch), pp. 15-54.

Mata y Martín, Ricardo (2001): *Delincuencia informática y Derecho penal*, (Madrid, Edisofer).

Matellanes Rodríguez, Nuria (2008): "Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)", *Revista Penal* nº 22, 2008, pp. 50-68.

Matellanes Rodríguez, Nuria (2009): "Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)", *Revista Penal* nº 23, 2009, pp. 52-72.

Mayo Calderón, Belén (2016): "Capítulo 17. Delitos contra el patrionio y contra el orden socioeconómico. III. Delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores y a la sustracción de cosa propia a su utilidad social o cultural", en Romeo Casabona, Carlos, Sola Reche, Esteban, Boldova Pasamar, Miguel Ángel (coordinadores): *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, (Granada, Comares), pp. 398-432.

Mestre Delgado (2019): "Tema 13. Delitos contra el patrimonio y contra el orden socioeconómico", en Lamarca Pérez, Carmen coordinadora: *Delitos, La parte especial del Derecho penal,* 3ª ed., (Madrid, Colex), pp. 341-566.

Mir Puig, Carlos (2002): "Sobre algunas cuestiones relevantes del derecho penal en internet", en López Ortega, Juan José (director): *Internet y Derecho penal*, Cuadernos de Derecho Judicial, (Madrid, Consejo General del Poder Judicial), pp. 281-304.

Miró LLinares, Fernando (2010): "Delitos informáticos. Hacking. Daños", en Ortiz de Urbina Gimeno, Íñigo (coordinador): *Memento Experto. Reforma Penal 2010*, *Ley Orgánica 5/2010,* (Madrid, Ediciones Francis Lefebvre), pp. 141-167.

Miró LLinares, Fernando (2016): «Cibercrímenes económicos y patrimoniales», en Ayala Gómez, Ignacio y Ortiz de Urbina Gimeno, Íñigo (coordinadores): *Memento Práctico Penal Económico y de la Empresa*, (Madrid, Francis Lefebvre).

Miró LLinares, Fernando (2012): *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, (Madrid, Marcial Pons).

Möhrenschlager, Manfred (1992): "El nuevo Derecho penal informático en Alemania", en Mir Puig, Santiago (coordinador): *Delincuencia informática*, (Barcelona, PPU), pp. 99-144.

Möhrenschlager, Manfred (1986), «Das neue Computerstrafrecht», *Wistra*, 1986, pp. 128-142.

Morales García, Oscar (2010): "Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248", en Quintero Olivares, Gonzalo (director): *La reforma penal de 2010: análisis y comentarios*, (Pamplona, Thomson Reuters Aranzadi) pp. 181-194.

Morales Prats, Fermín (2016)*:* "Artículo 197 bis", en Quintero Olivares, Gonzalo (director), Morales Prats, Fermín (coordinador): *Comentarios al Código Penal Español, Tomo I (Artículos 1 a 233),* 7ª ed, (Pamplona, Thomson Reuters Aranzadi), pp. 1475-1484.

Morón Lerma, Esther (2007): "Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos", *Delito e informática: algunos aspectos*, *Cuadernos penales José María Lidón*, número 4, (Bilbao, Universidad de Deusto), pp. 85-128.

Morón Lerma, Esther (2002): *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, 2ª ed., (Pamplona, Aranzadi).

Muñoz Conde, Francisco (2019): *Derecho penal, Parte Especial*, 22ª ed., revisada y puesta al día con la colaboración de Carmen López Pelegrín, (Valencia, Tirant lo blanch).

Navarro Frías, Irene (2016): "Capítulo 16. Delitos contra el patrimonio y el orden socioeconómico. II. Defraudaciones, insolvencias punibles, alteración de precios en concursos y subastas públicas y daños", en Romeo Casabona, Carlos, Sola Reche, Esteban, Boldova Pasamar, Miguel Ángel (coordinadores): *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, (Granada, Comares), pp. 359-396.

Pérez-Sauquillo Muñoz, Carmen (2019): *Legitimidad y técnicas de protección penal de bienes jurídicos supraindividuales*, (Valencia, Tirant lo Blanch).

Piqueres Castellote, Francisco (2006): "Conocimientos básicos en internet y utilización para actividades ilícitas", en Velasco Núñez, Eloy (director): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Cuadernos de Derecho Judicial, (Madrid, Consejo General del Poder Judicial), pp. 41-90.

Puente Aba, Luz María (2004): "Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?", en Faraldo Cabana, Patricia, Puente Aba, Luz María, Brandariz García, José Ángel (coordinadores): *Nuevos retos del Derecho penal en la era de la globalización*, (Valencia, Tirant lo blanch), pp. 381-410.

Queralt Jiménez, Joan (2015): *Derecho penal español, Parte Especial*, 7ª ed. revisada y actualizada con las Leyes Orgánicas 1/2015 y 2/2015, de 30 de marzo, 1ª ed. en la Editorial Tirant lo blanch, (Valencia, Tirant lo blanch).

Renobell Santaren, Víctor (2019), «Hacktivismo digital: de la cultura hacker a los delitos digitales», en Mallada Fernández, Covadonga (directora): *Nuevo retos de la ciberseguridad en un contexto cambiante*, (Pamplona, Thomson Reuters Aranzadi), pp. 237-261.

Ribagorda Garnacho, Arturo (2008): "La protección de datos personales y la seguridad de la información", *Revista Jurídica de Castilla y León*, nº 16, pp. 373-399.

Ribagorda Garnacho, Arturo (1996): "Seguridad de las tecnologías de la información", en Gallardo Ortiz, Miguel Ángel (director) : *Ámbito jurídico de las tecnologías de la información*, *Cuadernos de Derecho Judicial*, (Madrid, Consejo General del Poder Judicial), pp. 307-318.

Rodríguez Mourullo, Gonzalo, Alonso Gallo, Jaime y Lascuraín Sánchez, Juan Antonio (2001): "Derecho penal e internet", en Fernández Ordóñez, Miguel, Cremades García, Javier y Illescas Ortiz, Rafael (coordinadores): *Régimen jurídico de internet*, (Madrid, Editorial La Ley), pp. 257-310.

Romeo Casabona, Carlos Mª (2006): "De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal", en Romeo Casabona, Carlos Mª (coordinador): *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, (Granada, Comares), pp. 1-43.

Romeo Casabona, Carlos Mª (2016): "Capítulo 12. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", en Romeo Casabona, Carlos, Sola Reche, Esteban, Boldova Pasamar, Miguel Ángel (coordinadores): *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, (Granada, Comares), pp. 253-286.

Romeo Casabona, Carlos Mª (1988): *Poder informático y seguridad jurídica. «La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información»*, (Madrid, Fundesco).

Rueda Martín, Mª Ángeles (2018): *La nueva protección de la vida privada y de los sistemas*

de información en el Código penal, (Barcelona, Atelier).

Rueda Martín, Mª Ángeles (2001): *La Teoría de la imputación objetiva del resultado en el delito doloso de acción. (Una investigación, a la vez, sobre los límites ontológicos de las valoraciones jurídico-penales en el ámbito de lo injusto)*, (Barcelona, J. Mª Bosch).

Santana Vega, Dulce María (2000), *La protección penal de los bienes jurídicos colectivos*, (Madrid, Dykinson).

Salom Clotet, Juan (2006), "Delito informático y su investigación", en Velasco Núñez, Eloy (director): *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Cuadernos de Derecho Judicial, (Madrid, Consejo General del Poder Judicial), pp. 91-130.

Schünemann, Bernd (2000): "Kommentar zur § § 202a", en Jähnke, Burkhard, Laufhütte, Laufhütte y Odersky, Walter (editores): *Leipziger Kommentar Großkommentar*, 11ª Auf., (Berlin, Walter de Gruyter).

Sieber, Ulrich (1998): "Legal Aspects of Computer-Related Crime in the Information Society —Comcrime-Study—, prepared for the European Commission by Frof. Dr. Ulrich Sieber", disponible en http://www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

Sieber, Ulrich (1977): *Computerkriminalität und Strafrecht,* 1ª ed., (Munich, Heymann).

Soto Navarro, Susana (2003): *La protección penal de los bienes colectivos en la sociedad moderna*, (Granada, Comares).

Stree/Hecker (2019), "Kommentar zur § 303b", en Schönke, Adolf, Schröder, Horst, Eser, Albin *et alium* (autores): *Strafgesetzbuch Kommentar*, 30 Auf., (München, C. H. Beck).

Terradillos Basoco, Juan (1981): "La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal", *Revista de la Facultad de Derecho de la Universidad Complutense*, número 63, pp. 123-150.

Tomás y Valiente Lanuza, Mª Carmen (2015): "Artículo 197", en Gómez Tomillo, Manuel (director): *Comentarios prácticos al Código penal. Los delitos contra las personas, artículo 138-233*, Tomo II, 1ª ed., (Madrid, Thomson Reuters Aranzadi), pp. 653-672.

Wolf, Hagen (2008), "§ 303b", en Laufhütte, Rissing-van Saan, Tiedemann (coordinadores): *Strafgesetzbuch. Leipziger Kommentar Großkommentar*, Band 10, 12 Auflage, (Berlin, De Gruyter), pp. 416-437.

Zaczyk, Rainer (2017), "§ 303b", en Kindhäuser, Urs, Neumann, Ulfrid y Paeffgen, Hans-Ullrich (coordinadores): *NomosKommentar Strafgesetzbuch*, Band 3, 5 Auflage, (Baden-Baden, Nomos Verlagsgesellschaft), pp. 1598-1606.