universidad de león

FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2020 / 2021

EL DELITO DE HACKING O INTRUSISMO INFORMÁTICO (ART. 197 BIS.1 CP)

HACKING CRIME OR COMPUTER INTRUSION (ARTICLE 197 BIS.1 CC)

MÁSTER EN ABOGACÍA

AUTOR/A: D. MARÍA ENCINA MIRANDA LÓPEZ

TUTOR/A: D. MARÍA A. TRAPERO BARREALES

ÍNDICE

ÍNDICE DE ABREVIATURAS

AAVV	Autores Varios
AJEE	Anuario Jurídico y Económico escurialense (citado por número y año)
art./s	artículo/s
CCAA	Comunidades Autónomas
CE	Constitución española
CENDOJ	Centro de Documentación Judicial
coord./s	coordinador/es
CP	Código Penal
DI	Derecho Informático
dir./s	director/es
DNI	Documento Nacional de Identidad
DP	Derecho Penal
ed./s	editor/es
EM	Estados miembros
FGE	Fiscalía General del Estado
IDP	Revista de Internet, Derecho y Política (citada por número y año)
IP	Internet Protocol o Protocolo de Internet
LAJ	Letrado de la Administración de Justicia

LCDCE	Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, de 18 de octubre de 2007
LECrim	Ley de Enjuiciamiento Criminal, de 14 de septiembre de 1882
LL	Diario La Ley (citada por número y año)
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos, de 5 de diciembre de 2018
LOPJ	Ley Orgánica del Poder Judicial, de 1 de julio de 1985
LPI	Ley de Propiedad Intelectual, de 12 de abril de 1996
LSSI	Ley de Servicios de la Sociedad de la Información y de comercio electrónico, de 11 de julio de 2002
núm.	número
RBD	Revista Boliviana de Derecho (citada por número y año)
RCG	Revista de las Cortes Generales (citada por número y año)
RDPC	Revista de Derecho Penal y Criminología (citada por número y año)

REDUR	Revista Electrónica de Derecho de la Universidad de la Rioja (citada por número y año)
RICPC	Revista del Instituto de Ciencias Penales y Criminológicas (citada por número y año)
RPM	Revista Penal México (citada por número y año)
SAP	Sentencia de la Audiencia Provincial
STC	Sentencia del Tribunal Constitucional
STS	Sentencia del Tribunal Supremo
TC	Tribunal Constitucional
TIC’s	Tecnología de la información y de la comunicación
TS	Tribunal Supremo
UE	Unión Europea
VPN	Virtual Private Network

RESUMEN

La aparición y desarrollo de las TIC’s ha generado el surgimiento de una nueva fenomenología delictiva, que se engloba bajo el término de ciberdelitos. Uno de los delitos que se incluyen bajo esta expresión es el de intrusismo informático. El CP ha incluido esta modalidad delictiva, cumpliendo compromisos internacionales y de transposición de la normativa europea, en el Capítulo dedicado a los delitos de descubrimiento y revelación de secretos. A lo largo de este trabajo se llevará a cabo un análisis de los elementos configuradores de este delito, centrando la atención en el principal y más decisivo elemento que guía la labor interpretativa, el bien jurídico protegido, de manera particular atendiendo a si la tipificación responde a la aparición de un nuevo bien jurídico necesitado de protección penal, la seguridad de los sistemas informáticos, o se trata simplemente de la protección de un viejo bien jurídico, la intimidad, frente a nuevas formas de ataque aparecidas con el desarrollo de las nuevas tecnologías.

PALABRAS CLAVE

Intrusismo informático, seguridad informática, confidencialidad informática, intimidad, acceso no autorizado, persona jurídica, funcionario público, perseguibilidad.

ABSTRACT

The emergence and development of new sources of information and media has generated the emergence of a new criminal phenomenology, which is encompassed under the term of cybercrime. One of the crimes included in this expression is computer intrusion. The Criminal Code has included this type of crime, in compliance with international commitments and the transposition of European regulations, in the Chapter dedicated to the crimes of discovery and disclosure of secrets. Throughout this paper an analysis of the elements that make up this crime will be carried out, focusing attention on the main and most decisive element that guides the interpretative work, the protected legal right, particularly considering whether the criminalization responds to the emergence of a new legal right in need of criminal protection, the security of computer systems, or whether it is simply the protection of an old legal right, privacy, against new forms of attack that have appeared within the development of new technologies.

KEY WORDS

Computer intrusion, computer security, computer confidentiality, privacy, unauthorized access, legal person, public official, prosecutability.

OBJETO DEL TRABAJO

El presente trabajo se va a centrar en el análisis del delito de intrusismo informático, concretamente, en el delito tipificado en el art. 197 bis.1 CP, centrando la atención en los elementos configuradores de esta figura delictiva (el tipo penal).

Para llegar a entender este delito, y si su incursión en el CP es acertada y justificada, se debe realizar el estudio de los diferentes elementos típicos que configuran esta figura delictiva:

En primer lugar, como elemento central, se debe explicar el bien jurídico o bienes jurídicos que puede abarcar este delito y su forma de protección. Se trata de averiguar si se pretende proteger un bien jurídico que ha aparecido con el desarrollo de las TIC's o si, por el contrario, la razón de su incriminación obedece a que se está simplemente ante nuevas formas de ataque, con características específicas y más peligrosas, de los "tradicionales" bienes jurídicos.

En segundo lugar, se abordará el análisis de los sujetos, activo y pasivo, del delito de intrusismo informático. Merece especial atención el sujeto activo, pues para su configuración habrá de estarse a varios elementos que están conectados entre sí, esto es, el sujeto propiamente dicho, atendiendo a la descripción legal, y la falta de autorización para la realización de las conductas que describen esta figura delictiva. La explicación se completará con la exposición sobre la responsabilidad penal de las personas jurídicas, por un lado, y la previsión de un tipo penal cualificado referido al funcionario público, por otro lado.

En tercer lugar, se analizarán las conductas típicas que describen esta figura delictiva, tomando en consideración que se trata de un delito mixto alternativo: acceso, facilitar el acceso, permanecer en el sistema contra la voluntad de su titular.

En cuarto lugar, se entrará a valorar el cambio de referencia del objeto material del delito, pues si en la reforma de 2010 este eran los datos o programas contenidos en un sistema informático, a partir de la reforma de 2015 el objeto material es el propio sistema informático. Este cambio ha de ser analizado con cierto detenimiento, pues tiene consecuencias, tanto en la formulación del bien jurídico protegido como en el momento consumativo del delito de intrusismo informático.

En quinto lugar, se valorará la previsión del tipo agravado o cualificado referido a la comisión del delito en el seno de una organización o grupo criminal, en concreto, entrando a explicar

el fundamento de esta circunstancia de agravación, por un lado, y a la exégesis propiamente dicha de los elementos que configuran esta circunstancia cualificante, por otro lado.

Por último, se hará una mención especial a la perseguibilidad del delito y su especial dificultad, centrando la atención en dos de los aspectos que llevan a extraer esta conclusión, la primera, el anonimato del autor que ofrece Internet, la segunda, la frecuencia con que los delitos cibernéticos se cometen en un determinado país y tienen efectos en otro u otros territorios, con las consecuencias que de ello se derivan a la hora de establecer la competencia para el conocimiento de estos hechos delictivos.

METODOLOGÍA

En cuanto a la metodología empleada en la elaboración de este trabajo, es la que corresponde a un trabajo de tipo jurídico, en concreto de ámbito jurídico-penal, donde se debe recurrir al estudio y análisis dogmático, pero en el que se tienen en cuenta consideraciones de política criminal. Es, en definitiva, el método que tiene como primer precursor al Profesor Roxin, en la doctrina alemana, método que ha sido seguido por varios penalistas en la doctrina española, entre otros, los integrantes de la escuela científica encabezada por el Profesor Luzón Peña. Las consideraciones de política criminal se han de tomar en consideración teniendo muy presente que se está ante una investigación jurídico-penal, donde el principio de legalidad en la labor exegética tiene un papel fundamental que no puede ser olvidado.

En el punto dedicado a la metodología es frecuente también hacer una breve referencia a las principales fases de desarrollo este trabajo, que se pueden estructurar de la siguiente forma.

En primer lugar, se procedió a la elección de la tutora, Dra. María A. Trapero Barreales, y del tema objeto del trabajo, el delito de intrusismo informático, en concreto el art. 197 bis.1 CP.

En segundo lugar, se realizó una búsqueda exhaustiva de bibliografía a través de las plataformas proporcionadas por la Universidad y a través de Dialnet, también se consultaron diversas páginas web con el objetivo de enfocar y aclarar el tema elegido. En la búsqueda bibliográfica se ha tenido que hacer una selección de los trabajos más relevantes, tanto de la versión dada en la reforma de 2010 como en la de 2015, pues, aunque la historia de este delito es muy corta, pues como se ha dicho se incluye por primera vez en el CP en la reforma de 2010, sin embargo, el número de trabajos dedicados a su estudio es muy abundante. Para la búsqueda de jurisprudencia recurrí a la plataforma Aranzadi y CENDOJ, seleccionando sobre todo la más reciente.

En tercer lugar, tras la selección de la bibliografía (manuales, comentarios a las reformas de 2010, comentarios al CP, monografías, artículos) y de la jurisprudencia, se procedió a su sistematización y lectura comprensiva. Tras la lectura de las principales obras se elaboró el primer borrador de índice, para su aprobación y supervisión por la tutora del trabajo.

Y, en último lugar y conectada con la fase anterior, la redacción del trabajo, con la supervisión de la tutora y revisiones posteriores hasta la obtención del visto bueno.

El sistema de citas utilizado ha sido el recomendado por la tutora del trabajo, para las citas a nota de pie de página se ha optado por la información más sintética pero necesaria para la localización del trabajo citado, dejando para el índice de bibliografía consultada la información completa.

I. INTRODUCCIÓN

En la actualidad se puede observar que cuanto mayor es el desarrollo de una sociedad, mayor dependencia se tiene de las TIC's [1]. Internet es un gran mecanismo para intercambiar datos e información, tiene incidencia en muchos aspectos de la vida, en la economía, la política, las relaciones sociales e, inclusive, en el Derecho[2].

Es incuestionable que el desarrollo de las nuevas TIC's, sobre todo el desarrollo de las redes de transmisión de datos, es decir, Internet, han planteado riesgos concretos para la garantía de determinados intereses que se deben salvaguardar[3].

En efecto, la expansión y generalización de Internet ha provocado la aparición de un elenco de actividades nocivas para los ciudadanos, algunas de las cuales producen lesiones en los bienes jurídicos relevantes protegidos por el DP[4].

La ciberdelincuencia es un término que puede ser utilizado en un sentido amplio, esto es, para abarcar los supuestos en los que se utiliza Internet como entorno donde son atacados los propios sistemas de información y redes electrónicas o sus archivos y programas, y también para referirse a los supuestos en los que se convierte en un medio comisivo de múltiples actividades ilícitas[5]. La UE ha definido la ciberdelincuencia como las actividades delictivas realizadas con la ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas; en concreto, con este término se engloban los tres tipos de conductas que se van a mencionar a continuación[6]:

---

[1] FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 89-90.

[2] ASENCIO GALLEGO, en: ASENCIO MELLADO (dir.)/FERNÁNDEZ LÓPEZ (coord.), *Justicia penal y nuevas formas de delincuencia*, 2017, 44.

[3] DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 16; PÉREZ ESTRADA, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 306-307; VIDAURRI ARÉCHIGA, en: NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 198.

[4] DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 18; MORALES GARCÍA, en: QUINTERO OLIVARES (dir.), *La Reforma Penal de 2010: Análisis y Comentarios*, 2010, 182; RAYÓN BALLESTEROS/GÓMEZ HERNÁNDEZ, *AJEE* 47 (2014), 211; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 29.

[5] Sobre este concepto amplio de ciberdelincuencia o ciberdelitos, BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 35.

[6] Sobre esta triple clasificación utilizada en la UE, ALMENAR PINEDA, *El delito de hacking*, 2018, 32.

- Las formas tradicionales de actividades delictivas, pero utilizando Internet para cometer tales delitos.
- La publicación de contenidos ilegales, como material que incite al terrorismo, la violencia, el racismo o la xenofobia o la pornografía infantil.
- Delitos específicos de las redes electrónicas, que incluyen nuevos delitos, a menudo de amplia variedad y a gran escala, desconocidos antes de Internet. Los delincuentes atacan sistemas de información, en ocasiones amenazando infraestructuras críticas de un Estado, por lo que la amenaza se dirige también a sus ciudadanos.

El avance de Internet y la existencia de nuevos delitos que se pueden cometer a través de él han dado lugar al surgimiento de una nueva rama o sector normativo, el Derecho Informático. Dentro del DI, se encontraría el DP Informático; el primer concepto se refiere al conjunto de normas jurídicas que regulan la utilización de bienes y servicios informáticos en la sociedad, el segundo concepto a los tipos penales que surgen para la protección de bienes jurídicos que son susceptibles de ser atacados a través de medios informáticos[7].

Los delitos que se cometen a través de Internet son los delitos informáticos. Podemos encontrar varias definiciones, por un lado, se definen como todos aquellos delitos cometidos a través del medio telemático y cuya vía probatoria se sustenta en la prueba informática[8], pero también se pueden entender como una serie de acciones y/u omisiones dolosas o imprudentes, sancionadas por ley, que se han cometido directa o indirectamente a través de un bien o servicio informático[9].

En efecto, se pueden distinguir dos grupos de delitos relativos a los sistemas informáticos, en primer lugar, están los delitos cuya finalidad es la protección de esos sistemas informáticos considerados como objeto material, y, en segundo lugar, están los delitos relacionados con la utilización de los sistemas informáticos con fines delictivos. Teniendo en cuenta esa

[7] Sobre estos conceptos, entre otros muchos, DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 22-23; ALMENAR PINEDA, *El delito de hacking*, 2018, 34.
[8] FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 156.
[9] VIDAURRI ARÉCHIGA, en: NAVA GARCÉS (coord.), *Ciberdelitos*, 2019, 204.

clasificación, el sistema informático en sí mismo puede ser considerado como bien jurídico protegido, pero también puede ser utilizado para lesionar otro bien jurídico protegido[10].

Por otro lado, también la delincuencia informática tiene una serie de características que la convierten en algo específico. ALMEDAR PINEDA[11] las enumera de la siguiente manera:

- Los delitos informáticos en general no tienen un bien jurídico común afectado.
- Mayor facilidad para llevar a cabo estos delitos, las pruebas no suelen ser contundentes y pueden manipularse con facilidad.

Más completa y precisa es la descripción de las características de los delitos informáticos realizada por DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN[12]. En concreto, para estos autores hay cuatro aspectos característicos:

- Se cometen fácilmente.
- Requieren escasos recursos en relación al perjuicio que causan.
- Pueden cometerse en una jurisdicción sin estar físicamente presente en el territorio sometido a la misma.
- Se benefician de las lagunas de punibilidad que pueden existir en determinados Estados, algunos de los cuales se han denominado paraísos cibernéticos, debido a su nula voluntad política de tipificar y sancionar estas conductas.

Con el surgimiento de los delitos informáticos o ciberdelitos ha aparecido también un nuevo grupo de delincuentes cibernéticos, los llamados hackers. En un principio, la noción de hacker alude a expertos informáticos, personas que se dedican a programar de forma entusiasta y creen que poner en común la información constituye un extraordinario bien y que, además, para ellos es un deber de naturaleza ética compartir su competencia y pericia elaborando software gratuito y facilitando el acceso a la información y a los recursos de computación siempre que ello sea posible[13].

---

[10] Así lo matizan, ORTS BERENGUER/BOIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 13-14; ALMENAR PINEDA, *El delito de hacking*, 2018, 106.
[11] ALMENAR PINEDA, *El delito de hacking*, 2018, 37-39.
[12] DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 80.
[13] Así lo afirman, entre otros, MATELLANES RODRÍGUEZ, *RICPC* XXVI (2005), 132; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 41.

A día de hoy, esa característica de la alta especialización informática como requisito para ser hacker se está poniendo en duda. En la actualidad, la mayoría no son expertos informáticos, simplemente tienen conocimientos básicos de informática, pero aprovechan programas y aplicaciones para realizar sus incursiones[14].

Los hackers utilizan técnicas para acceder, sin la debida autorización, a sistemas informáticos ajenos, tratan de vencer las claves informáticas de los accesos, es decir, de descubrir las lagunas de protección. Es por ello que muchas compañías los contratan para que, antes de instalar sus sistemas informáticos, los analicen para ver si presentan grietas por las que alguien se pueda colar[15].

A pesar de que la imagen de los hackers no es muy buena, disponen de una serie de normas conocidas, entre las cuales están[16]:

- No hacer daño intencionalmente.
- Modificar solo lo estrictamente necesario para entrar y evitar ser localizado.
- No hackear nunca por venganza, intereses personales o económicos, además de no comentar con nadie las acciones realizadas.

Hay tres tipos básicos de hacker[17]:

- Black hats: Poseen habilidades extraordinarias en informática, recurren a actividades maliciosas.
- White hats: También poseen grandes habilidades, pero utilizan sus habilidades con fines defensivos.
- Gray hats: Puede dedicarse tanto a actividades maliciosas como a usar sus habilidades con fines defensivos.

No puede identificarse al hacker como un cibercriminal. Por otro lado, no hay un único perfil de ciberdelincuente, hay múltiples. Por ello, al hablar de ciberdelincuente nos referimos a

[14] DÍEZ GÓMEZ, *REDUR* 8 (2010), 174; MIRÓ LLINARES, en: MIRÓ LLINARES/AGUSTINA SANLLEHÍ/MEDINA SARMIENTO/SUMMERS (eds.), *Crimen, oportunidad y vida diaria. Libro homenaje al Profesor Dr. Marcus Felson*, 2015, 434.
[15] ASENCIO GALLEGO, en: ASENCIO MELLADO (dir.)/FERNÁNDEZ LÓPEZ (coord.), *Justicia penal y nuevas formas de delincuencia*, 2017, 47.
[16] DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 103.
[17] Alude a estos tres tipos, GIMÉNEZ SOLANO, *Hacking y ciberdelito*, 2011, 75.

cualquier sujeto que delinque usando el ciberespacio como parte esencial o central del delito[18].

El acceso ilegítimo a un sistema informático para el hacker puede llegar a convertirse en un culto y hasta un deporte competitivo[19], pero, como se va a explicar a continuación, este tipo de comportamientos puede llegar a ser un hecho constitutivo de un ilícito penal: el delito de hacking o de intrusismo informático. Este delito pertenece indudablemente al denominado DP informático o cibernético, sea este concepto utilizado en sentido estricto o en sentido amplio.

II. EL DELITO DE HACKING O INTRUSISMO INFORMÁTICO (ART. 197 BIS.1 CP)

Este es un delito de reciente inclusión en el vigente CP, pues su tipificación se ha producido con la aprobación de la reforma operada, primero con la LO 5/2010, de 22 de junio, y segundo, con la LO 1/2015, de 30 de marzo.

Los motivos de su inclusión en el CP se encuentran, por un lado, en la ratificación del Convenio de Budapest de 23 de noviembre de 2001 sobre ciberdelincuencia del Consejo de Europa y, por otro lado, por la necesidad de adaptar el Derecho interno a la Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, sobre los ataques contra los sistemas de información, sustituida por la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información, ya que en ambos textos normativos se impone la necesidad de la creación de un delito de acceso ilegal a sistemas informáticos[20].

---

[18] MIRÓ LLINARES, en: MIRÓ LLINARES/AGUSTINA SANLLEHÍ/MEDINA SARMIENTO/SUMMERS (eds.), *Crimen, oportunidad y vida diaria. Libro homenaje al Profesor Dr. Marcus Felson*, 2015, 434; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 43.

[19] PALAZZI, en: DUPUY (dir.)/KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, 2018, 38.

[20] CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 249; MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 142; BOLEA BARDON, en: CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal. Reforma LO 5/2010*, 2011, 468; GIMÉNEZ SOLANO, *Hacking y ciberdelito*, 2011, 81-82; MORALES GARCÍA, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 152; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015,

Las conductas de intrusismo informático o hacking no se encontraban reguladas con anterioridad a la LO 5/2010; esto no quiere decir que quedaran completamente impunes. Es decir, si el intrusismo informático era el medio para cometer otra infracción, la sanción de esa infracción comprendería el acceso al sistema de información[21].

La propuesta de regular de manera autónoma y específica las conductas de hacking se ha cumplido con las dos reformas anteriormente citadas, pues se ha reconocido que el intrusismo informático por sí mismo es un grave atentado a intereses que han de ser objeto de protección penal, como se va a explicar a continuación en el apartado relativo al bien jurídico protegido[22].

1. Bien jurídico protegido

Como es sabido, el DP tiene como misión principal la protección de bienes jurídicos a través de la prevención[23]. El concepto de bien jurídico se puede definir como referido a las condiciones necesarias para el desarrollo de la vida del individuo y de la sociedad, o más concretamente, para el desarrollo de la vida de la persona, como individuo en su esfera más íntima y para su desarrollo en sociedad[24]. Para que una acción pueda considerarse delito es necesario que infrinja un determinado orden de la comunidad o un elemento valioso de la vida social; solo así se estaría cumpliendo con uno de los principios limitadores del *ius puniendi*, el de exclusiva protección de bienes jurídicos o principio de lesividad[25].

En la explicación sobre el bien jurídico objeto de protección por una determinada figura delictiva ha de estarse, inicialmente al menos, a la ubicación sistemática de la correspondiente

671; GONZÁLEZ COLLANTES, *RDPC* 13 (2015), 73; ASENCIO GALLEGO, en: ASENCIO MELLADO (dir.)/FERNÁNDEZ LÓPEZ (coord.), *Justicia penal y nuevas formas de delincuencia*, 2017, 49.

[21] Así lo advierte, por todos, ALMENAR PINEDA, *El delito de hacking*, 2018, 161-162.

[22] CASTELLÓ NICÁS, en: MORILLAS CUEVA (dir.), *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, 2015, 505; ALMENAR PINEDA, *El delito de hacking*, 2018, 162; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 174-175.

[23] LUZÓN PEÑA, *Lecciones de Derecho Penal. Parte general*, 3ª, 2016, 13.

[24] LUZÓN PEÑA, *Lecciones de Derecho Penal. Parte general*, 3ª, 2016, 169.

[25] RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 365; ALMENAR PINEDA, *El delito de hacking*, 2018, 108.

modalidad delictiva[26]. El art. 197 bis.1 CP está ubicado en el Título X del Libro II del CP, en los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Más concretamente, en su Capítulo I, dedicado al descubrimiento y revelación de secretos.

Con la reforma de la LO 5/2010, el hacking se tipifica dentro del mismo precepto de otros delitos contra la intimidad, en concreto, en el art. 197.3 CP; tras la reforma de la LO 1/2015, la regulación del intrusismo informático se realiza en un precepto autónomo, el art. 197 bis.1 CP, lo que puede servir también para configurar un bien jurídico específico, aunque esté relacionado con la intimidad[27].

El legislador en el Preámbulo de la LO 1/2015 explica que se introduce una separación nítida entre los supuestos de revelación de datos que afectan directamente a la intimidad personal, y el acceso a otros datos o informaciones que puedan afectar a la privacidad pero que no están referidos directamente a la intimidad personal. Aunque el legislador haga referencia a una separación nítida entre los delitos que afectan directamente a la intimidad personal y el acceso a datos o informaciones que no están referidos directamente a la intimidad personal, ha de advertirse que todos los tipos penales están en el mismo Capítulo, el dedicado a los delitos de descubrimiento y revelación de secretos[28].

Esta ubicación sistemática abre el interrogante de si la intimidad constituye o no el objeto de protección en el delito de intrusismo informático. Para responder a esta cuestión se deberá analizar previamente el objeto de tutela común en los delitos contra la intimidad, a fin de poder precisar si el art. 197 bis.1 CP cumple o no con esa misma estructura[29].

El derecho a la intimidad, bien jurídico protegido en este Capítulo I, es un derecho fundamental que se encuentra en el art. 18 CE. Esto significa que le acompañan todas las

[26] RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 360; ALONSO GARCÍA, *Derecho penal y redes sociales*, 2015, 335; ALMENAR PINEDA, *El delito de hacking*, 2018, 105-111; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 253; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 26.
[27] ALMENAR PINEDA, *El delito de hacking*, 2018, 111.
[28] CASTELLÓ NICÁS, en: MORILLAS CUEVA (dir.), *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, 2015, 505; ALMENAR PINEDA, *El delito de hacking*, 2018, 111; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 91-92.
[29] ALMENAR PINEDA, *El delito de hacking*, 2018, 111-112; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 26.

garantías constitucionales de tutela de esos derechos, especialmente las relativas a la reserva de LO, su tutela ante los tribunales ordinarios por un procedimiento preferente y sumario y ante el TC a través del recurso de amparo[30].

El derecho a la intimidad no se concibe solo como un derecho de exclusión de terceros sobre la información personal, también se incluye el aspecto positivo de poder controlar los datos personales que circulan a través de los sistemas informáticos[31].

El reconocimiento del derecho a la intimidad personal y familiar tiene por objeto garantizar al individuo un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, ya sean poderes públicos o particulares. Se vulnera el derecho a la intimidad cuando se desvelan datos pertenecientes a la esfera privada y de exclusión del conocimiento de los demás. El TC ha reconocido este derecho como autónomo a pesar de su relación con el derecho al honor y a la propia imagen, dirigidos todos ellos a la protección del patrimonio moral de los individuos[32].

En el ámbito penal, como ya se ha indicado, el Título X del Libro II del CP se centra en las conductas que pueden atentar contra la intimidad. El Capítulo I "Del descubrimiento y revelación de secretos" agrupa los arts. 197 a 201[33].

La ubicación del delito de intrusismo informático o hacking en los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio ha generado numerosas críticas, ya que se entiende que no necesariamente se tutela el derecho a la intimidad[34].

---

[30] ALMENAR PINEDA, *El delito de hacking*, 2018, 112-114.

[31] La STC núm. 254/1993, de 20 de julio, analiza el derecho a la intimidad desde un punto de vista negativo, considerándolo como un derecho de exclusión de los terceros sobre los datos personales, y desde un punto de vista positivo, comprendiendo la existencia de ficheros con datos personales, sus fines y los responsables de los mismos. Sobre los dos aspectos del derecho fundamental, véase, entre otros, MORALES PRATS, *La tutela penal de la intimidad: privacy e informática*, 1984, 123-124; ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 21; ALMENAR PINEDA, *El delito de hacking*, 2018, 112-114.

[32] Sobre este bien jurídico de la intimidad, véase, entre otros, RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 21; FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 137.

[33] RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 27-28; RUEDA MARTÍM, *Indret* 4 (2013), 12; ALMENAR PINEDA, *El delito de hacking*, 2018, 112.

[34] De esta opinión, entre otros, CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 249-250; RUEDA MARTÍN, en: ROMEO

En la discusión relativa al bien jurídico protegido en el delito de intrusismo informático se pueden diferenciar al menos tres posturas teóricas[35]:

- Seguridad informática: se trata de un bien jurídico de naturaleza colectiva, no disponible individualmente, cuya protección evita la lesión de otros bienes jurídicos de naturaleza individual o incluso supraindividual[36].
- Integridad y disponibilidad de los sistemas informáticos: se parte de la informatización de todos los datos, la confianza en su autenticidad y en que se podrá disponer de ellos con el empleo de nuevas tecnologías como bien jurídico protegido[37].
- Intimidad: la autodeterminación informática o habeas data, se concibe como el derecho que tienen los ciudadanos a decidir si se difunde su información personal y familiar y además en qué forma se difunde. Es decir, se trata del poder de control que tiene todo individuo sobre su información. La intimidad informática se plantea como un bien jurídico autónomo y diferenciado, de naturaleza estrictamente informática, merecedor y necesitado de protección penal[38]. El

CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 363; GONZÁLEZ COLLANTES, *RDPC* 13 (2015), 72; ALMENAR PINEDA, *El delito de hacking*, 2018, 112; TOMÁS-VALIENTE LANUZA, *IDP* 27 (2018), 38; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 26.

[35] Así lo señalan, entre otros, HERNÁNDEZ DÍAZ, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 45-47; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 46-48; MORALES GARCÍA, en: QUINTERO OLIVARES (dir.), *La Reforma Penal de 2010: Análisis y Comentarios*, 2010, 184; MORALES GARCÍA, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 153; ALMENAR PINEDA, *El delito de hacking*, 2018, 118-119; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 91.

[36] Los bienes jurídicos protegidos de naturaleza individual son el honor e intimidad personal, patrimonio o libertad sexual, etc. mientras que los bienes jurídicos de naturaleza supraindividual son la seguridad estatal, orden público o paz pública, HERNÁNDEZ DÍAZ, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 45; ALMENAR PINEDA, *El delito de hacking*, 2018, 119; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 46.

[37] HERNÁNDEZ DÍAZ, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 45-47; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 46-48; MORALES GARCÍA, en: QUINTERO OLIVARES (dir.), *La Reforma Penal de 2010: Análisis y Comentarios*, 2010, 184; MORALES GARCÍA, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 153; ALMENAR PINEDA, *El delito de hacking*, 2018, 118-119.

[38] HERNÁNDEZ DÍAZ, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 47; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 47-48.

hecho de saltarse las barreras de seguridad informáticas, se considera un atentado contra el derecho a la intimidad informática[39].

Para varios autores como RUEDA MARTÍN, ALMENAR PINEDA, COLÁS TURÉGANO, GONZÁLEZ COLLANTES y CARRASCO ANDRINO, entre otros[40], el bien jurídico protegido del art. 197 bis.1 CP es la seguridad de los sistemas informáticos, que comprende la confidencialidad, integridad y disponibilidad de este sistema (y sería el primer aspecto el que principalmente sería objeto de protección por el delito de intrusismo informático). En el caso de BARRIO ANDRÉS[41] considera que el bien jurídico protegido es la intimidad de los sistemas informáticos.

Sin embargo, para ALONSO GARCÍA[42], los bienes jurídicos protegidos en este delito pueden ser ambos, tanto la intimidad como la seguridad informática. El acceso no consentido a un sistema informático puede atentar contra la seguridad informática, en el sentido de poner en peligro el propio sistema; y también puede atentar contra la intimidad, ya que el equipo informático de una persona puede considerarse como un ámbito reservado de la misma.

Al hilo de la discusión sobre el bien jurídico protegido se plantea la cuestión de si la ubicación del delito del art. 197 bis CP es la adecuada o necesitaría establecerse en un título distinto, un nuevo título dedicado exclusivamente a los delitos informáticos, junto con el delito de daños informáticos del art. 264 CP, el delito de obstaculizar o interrumpir el funcionamiento de sistemas informáticos del art. 264 bis CP y el delito de producir, facilitar o importar

[39] BARRIO ANDRÉS, RCG 83 (2011), 286; BARRIO ANDRÉS, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 40; *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 90.

[40] De esta opinión, entre otros, CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 251; RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 373; BOLEA BARDON, en: CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal. Reforma LO 5/2010*, 2011, 469; CASTELLÓ NICÁS, en: MORILLAS CUEVA (dir.), *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, 2015, 505; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 676; GONZÁLEZ COLLANTES, *RDPC* 13 (2015), 72; ALMENAR PINEDA, *El delito de hacking*, 2018, 139.

[41] BARRIO ANDRÉS, *Ciberdelitos: amenazas criminales del ciberespacio*, 2017, 67.

[42] ALONSO GARCÍA, *Derecho penal y redes sociales*, 2015, 338.

programas para cometer esos delitos del art. 264 ter CP o, inclusive, si hubiera sido preferible la creación de una ley penal especial[43].

En el Preámbulo de la LO 1/2015, el legislador opta por mantener este delito en el Título dedicado a los delitos contra la intimidad, pero decide que su regulación ha de hacerse en un precepto específico, el art. 197 bis.1 CP, para entender que estas conductas, aunque pueden afectar a la privacidad, no se refieren directamente a la intimidad[44]. Con esta referencia el legislador de 2015 parece querer dar carta de naturaleza a la tesis que defiende que en el delito de intrusismo informático no se pretende proteger un bien jurídico relacionado con la intimidad.

Teniendo en cuenta lo anteriormente explicado, las dos mejores opciones para formular el bien jurídico protegido del delito de hacking son la intimidad y la seguridad de los sistemas informáticos.

La intimidad como bien jurídico protegido del art. 197 bis.1 CP debería ser tenida en cuenta en el contexto actual, adaptándose a las nuevas tecnologías y a las relaciones de las personas a través y con los sistemas informáticos. Además, parece ser el bien jurídico protegido establecido por el legislador de 2010, ya que, aparte de tipificar la conducta en el art. 197.3 CP, por tanto, en el mismo título que los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, decidió incluirla dentro del mismo Capítulo dedicado al descubrimiento y revelación de secretos, en un apartado dentro del art. 197 CP, el delito que indiscutiblemente protege este bien jurídico. Sin embargo, el legislador de 2015 ha decidido regular la conducta del hacking en un precepto propio, aunque se mantiene en el mismo Capítulo, sin desvincularlo completamente por tanto de los delitos contra la intimidad[45].

[43] De esta opinión, entre otros, ALMENAR PINEDA, *El delito de hacking*, 2018, 119-130; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 253; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 26.
[44] Así también lo pone de relieve ALMENAR PINEDA, *El delito de hacking*, 2018, 120-121.
[45] Así lo matiza, ALMENAR PINEDA, *El delito de hacking*, 2018, 124-125.

En todo caso se ha considerado un acierto que el delito de intrusismo informático ya no aparezca como un apartado del art. 197 CP, sino que aparezca en un precepto separado e independiente, en el art. 197 bis.1 CP[46].

La STS de 24 de febrero de 2015[47] parece que se ha decantado por esta interpretación sobre el bien jurídico protegido en el delito de acceso ilícito a los sistemas de informáticos, pues afirma que, a pesar de que los datos contenidos en esos sistemas puedan parecer irrelevantes aisladamente, en su conjunto pueden ofrecer una descripción detallada de la personalidad del titular, lo que afecta a su intimidad.

Si se tiene en cuenta el Preámbulo y el texto articulado del Convenio de Budapest contra la ciberdelincuencia, en el que se expone que dicho Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, con esta terminología parece que se está haciendo referencia a varios bienes jurídicos que han de ser objeto de protección a través de diferentes delitos informáticos[48]: la confidencialidad, para garantizar la utilización del sistema solo por la persona autorizada; la integridad, o la utilización del sistema por la persona autorizada, sin que terceros introduzcan modificaciones de contenido de la información almacenada en el sistema; y la disponibilidad de los datos o sistemas informáticos, o el control sobre la utilización del sistema por parte de la persona autorizada. Con el delito de intrusismo se trataría de dar protección al primero de los bienes jurídicos.

La consideración de la confidencialidad, integridad y disponibilidad de los sistemas informáticos significa que cobra carta de naturaleza la aparición de nuevos bienes jurídicos, y su protección ha de ser objeto de atención por el DP atendiendo a las siguientes razones[49]:

- Interés en la seguridad de la utilización de las TIC's, sirviendo ese bien jurídico como barrera de contención para otros bienes jurídicos.
- Armonización legislativa con el derecho comparado y comunitario.

[46] De esta opinión, entre otros, ALMENAR PINEDA, *El delito de hacking*, 2018, 126-127.
[47] STS núm. 97/2015, 24 de febrero.
[48] Así lo destacan, entre otros, RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 373-374; ALMENAR PINEDA, *El delito de hacking*, 2018, 130-131.
[49] Sobre estos motivos, véase, ALMENAR PINEDA, *El delito de hacking*, 2018, 131.

- La informática es una fuente de peligro que necesita control, por sus repercusiones a otros bienes jurídicos, está legitimada la intervención del DP.

Se trataría de un bien jurídico distinto a la intimidad, ya que se considera que la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye el bien jurídico protegido[50].

Este es el criterio que parece seguir el legislador europeo de la DM 2005/222/JAI, y posteriormente en la Directiva 2013/40/UE, al referirse a la protección de los sistemas de información en los Considerandos 1, 2 y 26, imponiendo a los EM la adopción de medidas para proteger los sistemas de información. Por lo que se entiende que el bien jurídico protegido sería la seguridad de los sistemas de información, o los sistemas de información, un supraconcepto que englobaría como bienes jurídicos más específicos o concretos la confidencialidad, la disponibilidad y la integridad de los sistemas de información[51].

En mi opinión, el bien jurídico protegido del delito de hacking es la seguridad de los sistemas de información, que se concreta en la confidencialidad, integridad y disponibilidad, lo que supone una protección de manera indirecta de otros bienes jurídicos, como la intimidad. Es decir, el bien jurídico protegido seguridad de los sistemas de información abarca la protección de otros bienes jurídicos.

2. Sujetos del delito

Tanto si se toma en consideración el concepto de acción como si se hace una explicación atendiendo a la teoría general del delito, se llega a la conclusión de que al DP solo le interesa la conducta humana[52].

Con la expresión sujetos del delito, en la teoría jurídica del delito se hace referencia a dos de los aspectos o elementos del tipo penal: por un lado, el sujeto activo, o autor del hecho

[50] RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 373; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 672.
[51] ALMENAR PINEDA, *El delito de hacking*, 2018, 132; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 673-674; TOMÁS-VALIENTE LANUZA, *IDP* 27 (2018), 38.
[52] ALMENAR PINEDA, *El delito de hacking*, 2018, 167.

delictivo (utilizando este término en sentido estricto)[53], y, por otro lado, el sujeto pasivo del delito, expresión con la que se alude al titular del bien jurídico protegido.

2.1. Sujeto activo

Si se atiende al tenor literal del art. 197 bis.1 CP, desde esta perspectiva se ha de llegar a la conclusión de que el delito de intrusismo informático es un delito común, pues cualquier persona puede ser autora del hecho delictivo descrito en este precepto[54]. Ahora bien, hay que señalar que lo más normal es que quien realice la conducta típica de este delito tenga los conocimientos informáticos necesarios para llevar a cabo una conducta tecnológicamente compleja, al menos así ha de ser cuando las medidas de seguridad que han de ser vulneradas presentan un elevado grado de dificultad[55].

Nos encontramos, por tanto, ante un delito común, que puede cometer cualquier persona, pero se debe tener en cuenta que el delito de hacking tiene una modalidad especial en el art. 198 CP, que se refiere a los supuestos en los que el delito es llevado a cabo por una autoridad o funcionario público, fuera de los casos permitidos por la ley, sin mediar causa por delito y prevaliéndose de su cargo; este delito se trata de un delito especial impropio[56]. Más adelante se entrará a analizar este tipo penal especial.

Por otro lado, en la explicación sobre el sujeto activo del delito también ha de dejarse constancia de que este delito también puede ser cometido por una persona jurídica. Como se sabe, desde la reforma 2010 en el DP español se ha previsto la responsabilidad penal de las personas jurídicas, pero siguiendo el sistema de numerus clausus, esto es, solo se va a exigir dicha responsabilidad penal en aquellos delitos en los que se haya establecido de manera

---

[53] ALMENAR PINEDA, *El delito de hacking*, 2018, 168; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 15.

[54] Así lo afirman, entre otros, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 147; COLÁS TURÉGANO, *RBD* XXI (2016), 221; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 92; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 276; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 15.

[55] De esta opinión, entre otros, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 147; ALMENAR PINEDA, *El delito de hacking*, 2018, 168.

[56] Hace esta calificación ALMENAR PINEDA, *El delito de hacking*, 2018, 169.

expresa. Esto es lo que ha sucedido en el delito de intrusismo informático, a través del art. 197 quinquies CP. Más adelante se hará un análisis de este precepto penal.

2.2. Sujeto pasivo

El sujeto pasivo del delito puede ser cualquier persona, siempre y cuando sea el titular del conjunto o sistema informático sobre el que se lleva a cabo el acceso no autorizado[57].

En el antiguo art. 197.3 CP introducido en la reforma de la LO 5/2010, se planteaban los casos en los que el titular del sistema era una persona, pero los datos albergados en dicho sistema pertenecían a otra persona. Por lo que nos encontramos con dos situaciones, la primera, si la persona que accede al sistema es el titular de los datos, y por ende, del derecho de intimidad, quedaría impune si el sistema no contuviese datos de terceros; mientras que la segunda situación, sería el caso de un tercero que accede al sistema sin ser el titular del sistema ni de los datos guardados en dicho sistema, pero estaría cometiendo solo un delito con el titular de los datos del sistema, no con la persona que ostenta la titularidad de dicho sistema[58].

Pero con la reforma de la LO 1/2015, y el planteamiento de que el bien jurídico protegido puede considerarse la seguridad e integridad del sistema, se tratará de preservar este bien, con independencia de que el sistema contenga datos de un tercero o del titular del sistema[59].

---

[57] MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 147; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 92; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 277; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 15.

[58] ALMENAR PINEDA, *El delito de hacking*, 2018, 169; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 277; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 15.

[59] ALMENAR PINEDA, *El delito de hacking*, 2018, 170; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 278; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 15.

3. Conductas típicas

El art. 197 bis.1 CP tiene una estructura formada por tres acciones, acceder al sistema de información, facilitar a otra persona el acceso al sistema de información, y mantenerse dentro del sistema de información.

Para ciertos autores, se trata de un tipo mixto alternativo, pues está integrado por conductas de acceder, facilitar o mantenerse, fungibles entre sí, resultando indiferente que se realice una u otra o incluso todas, pues el delito seguirá siendo el mismo, y el hecho de realizar varias de las conductas típicas no significa que se vaya a cometer varias veces este delito[60].

Es necesario analizar separadamente lo establecido en este primer apartado del precepto para un mejor entendimiento de las conductas típicas de este delito.

3.1. Acceder al conjunto o una parte del sistema de información

Es importante el término "acceda", ya que es el verbo típico para calificar la conducta del art. 197 bis.1 CP. La amplitud de su significado permite meter dentro de ese término todo tipo de accesos, incluido el acceso remoto a través de Internet o utilizando la red interna de una empresa[61]. El acceso al sistema o parte de él comprende el software, hardware y el acceso al router[62].

Un ejemplo de uso de la red interna de una empresa lo tendríamos en la SAP Madrid de 27 de noviembre de 2017[63], donde los denunciados usaron el usuario y contraseña de una compañera para acceder a la red interna de la empresa para consultar datos personales propios, en el momento de la intromisión carecían de autorización ya que habían sido despedidos.

[60] De esta opinión, entre otros, CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 249; FERNÁNDEZ TERUELO, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, 2011, 199; SUÁREZ-MIRA RODRÍGUEZ/JUDEL PRIETO/PIÑOL RODRÍGUEZ, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 170; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 92.
[61] Véase, en este sentido, ALMENAR PINEDA, *El delito de hacking*, 2018, 172.
[62] BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 93.
[63] SAP Madrid núm. 895/2017, de 27 de noviembre.

El acceso puede ser de dos tipos, directo o remoto. El acceso directo se produce cuando se accede físicamente a un sistema informático ajeno, sorteando la clave de acceso al mismo. Se ha discutido si cualquier forma de descubrir la contraseña supone vulnerar las medidas de seguridad. Mientras que el acceso remoto se lleva a cabo mediante una red de telecomunicaciones pública o privada, este tipo de acceso es el más habitual entre las conductas de intrusismo informático, el problema es que es difícilmente perseguible cuando se realiza desde conexiones no protegidas o desde redes que facilitan el anonimato[64].

Para MIRÓ LLINARES[65], el hacking por su propia naturaleza solo podría realizarse a través de un acceso remoto. No se consideraría hacking el acceso directo, en la propia terminal y no autorizado al sistema.

Se debe recordar que en el antiguo art. 197.3 CP introducido por la LO 5/2010, se requería el acceso a datos o programas informáticos. Mientras que en el nuevo art. 197 bis.1 CP introducido por la LO 1/2015, solo es necesario el acceso a una parte o al conjunto de un sistema de información. No es necesario llegar a los datos o programas del sistema de información, es suficiente con el mero acceso a todo o a una parte de dicho sistema[66].

Al tratarse de un delito de resultado, y siendo necesario el acceso al conjunto o a una parte de un sistema de información, puede suceder que el sujeto no consiga saltarse las medidas a pesar de tener intenciones de hacerlo y aun habiendo iniciado la acción; en este caso habrá que castigar a través de las reglas de la tentativa inacabada. También puede suceder que el

[64] Un ejemplo de este tipo de redes que facilitan el anonimato seria la red Tor. Para más detalles, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 150-152; BOLEA BARDON, en: CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal. Reforma LO 5/2010*, 2011, 468; SUÁREZ-MIRA RODRÍGUEZ/JUDEL PRIETO/PIÑOL RODRÍGUEZ, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 170; BARRIO ANDRÉS, *Ciberdelitos: amenazas criminales del ciberespacio*, 2017, 69; *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 93-94.

[65] MIRÓ LLINARES, *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, 2012, 54.

[66] COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 676; ALMENAR PINEDA, *El delito de hacking*, 2018, 177; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 175.

sujeto sí consigue saltar las medidas de seguridad, pero no consigue acceder al sistema, en cuyo caso habrá que castigar apreciando las reglas de la tentativa acabada[67].

3.2. Facilitar a otro el acceso al conjunto o a una parte del sistema de información

La referencia "o facilite el acceso a otro" constituye una novedad incluida en la reforma de 2015[68].

A primera vista, la conducta de facilitar a otro el acceso al sistema de información no plantea ninguna duda desde el punto de vista gramatical, si se considera facilitar como "hacer fácil o posible la ejecución de algo". Sin embargo, puede generar problemas de confusión con las conductas del art. 197 ter CP[69].

El art. 197 ter CP expresa 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: un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o 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.

En este precepto está previsto facilitar a terceros la comisión del delito del art. 197 bis.1 CP, a simple vista, el art. 197 ter CP parece que se refiere a facilitar instrumentos concretos para el acceso, como un programa informático o una contraseña de ordenador; pero precisamente

---

[67] ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 31-32; ALMENAR PINEDA, *El delito de hacking*, 2018, 181.

[68] Esta novedad fue introducida con la enmienda 824 propuesta por el grupo Popular en el Congreso de los Diputados: las modificaciones propuestas pretenden superar las limitaciones de la regulación vigente para ofrecer respuesta a la delincuencia informática en el sentido de la Directiva 2013/40/UE. Véase, más ampliamente, ALMENAR PINEDA, *El delito de hacking*, 2018, 170; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 94; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 281.

[69] ALMENAR PINEDA, *El delito de hacking*, 2017, 397; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 16.

esa ambigüedad en cuanto a facilitar puede acarrear problemas de delimitación en la práctica entre estas conductas[70].

La inclusión de esta conducta de facilitar el acceso supone una tipificación expresa de actos de cooperación elevados a categoría de autoría[71]. En estos casos, se produce una ampliación de la autoría a supuestos que con anterioridad se habrían considerado como participación. Por ello, para estos casos concretos deberá entenderse que se ha de realizar un efectivo acceso al sistema de información, puesto que no tendría sentido la ampliación del ámbito punible si no tuviera lugar ese acceso[72].

3.3. Mantenimiento en el sistema de información en contra de la voluntad de quien tenga el legítimo derecho a excluirlo

El mantenimiento en un sistema informático en contra de la voluntad de quien tenga el legítimo derecho a excluirlo constituye una de las tres conductas previstas del art. 197 bis.1 CP.

Se puede hablar de un complemento a la conducta del acceso ilícito prevista en el mismo precepto para conseguir una completa protección del bien jurídico, de tal forma que se refiere a los supuestos en los que el acceso es inicialmente lícito, pero se produce una permanencia en el sistema que excede de lo autorizado. Existe la obligación de abandonar el sistema porque se pierde la autorización[73].

Es precisa una voluntad contraria del titular del sistema informático a que continúe el mantenimiento en dicho sistema, retirando así el permiso inicialmente concedido. Por motivos de coherencia, al igual que no puede haber dudas en cuanto al permiso para entrar

[70] SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 179-180; ALMENAR PINEDA, *El delito de hacking*, 2018, 171; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 16.
[71] ALMENAR PINEDA, *El delito de hacking*, 2018, 170.
[72] COLÁS TURÉGANO, *RBD* XXI (2016), 219; ALMENAR PINEDA, *El delito de hacking*, 2017, 398-399; TEVENET GUTIÉRREZ, *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, 2019, 16-17.
[73] Así lo afirma ALMENAR PINEDA, *El delito de hacking*, 2017, 445-446.

en el sistema de información, en el caso de la permanencia en el sistema deberá constar inequívocamente que ese permiso inicial ha sido retirado[74].

Uno de los problemas de interpretación del artículo se centrará en la exigencia o no de vulneración de medidas de seguridad en la permanencia en el sistema, aunque todo parece indicar que la redacción del precepto parece referirse tanto al acceso como al mantenimiento[75].

Por ello, se puede llegar a entender que el acceso legítimo se convierte en acceso ilegítimo precisamente porque el titular del sistema ha retirado el permiso; o, por otro lado, que el sujeto estando autorizado para el acceso, aproveche para llevar a cabo actuaciones diferentes a las que estaba legitimado, de tal manera que se produce la permanencia ilícita en el sistema durante el tiempo necesario para llevar a cabo dichas actuaciones. En consecuencia, si la denegación del permiso va acompañada de medidas de seguridad para impedir la continuación en el acceso, la nueva entrada dará lugar a la primera de las conductas del art. 197 bis.1 CP[76].

No se entiende que para la conducta de mantenimiento en el sistema de información no se haya previsto el castigo del hecho de facilitar la permanencia en el sistema. Mientras que para el acceso al sistema si se han previsto las conductas que puedan facilitar dicho acceso, en el caso del mantenimiento podría haberse previsto el castigo de facilitar o permitir la permanencia en el sistema de información en contra del que tenga el derecho legítimo a excluirlo[77].

[74] COLÁS TURÉGANO, *RBD* XXI (2016), 218-219; ALMENAR PINEDA, *El delito de hacking*, 2017, 447.
[75] ALMENAR PINEDA, *El delito de hacking*, 2017, 447-448.
[76] ALMENAR PINEDA, *El delito de hacking*, 2017, 448-450.
[77] ALMENAR PINEDA, *El delito de hacking*, 2017, 451.

3.4. Vulnerando las medidas de seguridad establecidas para impedirlo

La importancia de las medidas de seguridad en relación con el acceso significa que, si este no está protegido, la conducta no sería típica penalmente. Además, si el sistema está protegido quiere decir que su titular no quiere que sea accesible[78].

Se debe tener en cuenta que, al tratarse de un delito doloso, si el sujeto no tiene la voluntad de quebrantar las medidas de seguridad del sistema, la conducta sería atípica; a igual conclusión ha de llegarse en el caso de un acceso producido por un descuido o una negligencia[79].

Se debe mencionar que este requisito no aparece en la descripción del delito de intrusismo en el Convenio de Budapest ni en la Decisión Marco 2005/222/JAI como elemento o requisito típico de imperativa inclusión, sino que dejan a los Estados la decisión de si quieren o no incluir este elemento en la descripción del delito, para limitar así el ámbito aplicativo de esta figura delictiva. Pero la Directiva 2013/40/UE sí hace mención expresa a que el acceso se haya cometido con violación de una medida de seguridad[80].

Si atendemos a las conductas de hacking, tiene sentido entender las medidas de seguridad como las relativas a la seguridad lógica, más concretamente, las aplicaciones o herramientas informáticas dirigidas a evitar el hacking o acceso ilícito al sistema y a la información en él contenido[81].

---

[78] De esta opinión, entre otros, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 149; FERNÁNDEZ TERUELO, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, 2011, 199; BARRIO ANDRÉS, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 41; *Ciberdelitos: amenazas criminales del ciberespacio*, 2017, 69; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 677; *RBD* XXI (2016), 220; ALMENAR PINEDA, *El delito de hacking*, 2018, 178; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 285.

[79] Así lo advierten, DE LA MATA BARRANCO/HERNÁNDEZ DÍAZ, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 176-176; ALMENAR PINEDA, *El delito de hacking*, 2018, 178;

[80] ALMENAR PINEDA, *El delito de hacking*, 2018, 178; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 282-283.

[81] Véase, en este sentido, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 149; FERNÁNDEZ TERUELO, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, 2011, 199; ALMENAR PINEDA, *El delito de hacking*, 2018, 179; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 283.

Es decir, quedan excluidas las medidas que un usuario pueda haber establecido para un fin distinto al acceso, como un control de acceso al sistema que tiene la finalidad de verificarlo[82]. Tal es el caso de la SAP de Alicante de 16 de septiembre de 2015[83], donde se establecía que el acceso con clave que tiene un sujeto por su cargo no implica la vulneración de medidas de seguridad que exige el tipo, se trataría de un acceso no autorizado. El control de acceso que tienen que realizar los empleados no es más que un registro de los mismos que permite conocer los que se han verificado y la finalidad con la que se declaran hechos los accesos.

Esto nos plantea dudas sobre si se deben considerar otros tipos de medidas de seguridad, como pueden ser las medidas físicas, como, por ejemplo, una habitación cerrada con llave donde se encuentra el ordenador. La inclusión de medidas físicas en el concepto de medidas de seguridad resultaría menos problemática y no solo a las de naturaleza informática, siempre y cuando dichas medidas hayan sido establecidas para evitar el hacking[84].

3.5. Sin estar debidamente autorizado

Siguiendo con el análisis del tipo penal, para que el hecho constituya un ilícito penal el sujeto activo debe realizar cualquiera de las conductas antes mencionadas y "no estar debidamente autorizado"; en la redacción originaria de este delito en el antiguo art. 197.3 CP se utilizaba la expresión acceda sin autorización, la reforma introducida por la LO 1/2015 en el nuevo art. 197 bis.1 CP ha cambiado esta descripción por el término sin estar debidamente autorizado[85].

---

[82] Hacen esta aclaración MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 150; ALMENAR PINEDA, *El delito de hacking*, 2018, 179; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 285.

[83] SAP Alicante núm. 351/2015, de 16 de septiembre.

[84] Se deberá valorar las circunstancias en cada caso, para comprobar si la medida de seguridad estaba destinada a impedir el acceso al sistema. Así lo afirman, entre otros, ALMENAR PINEDA, *El delito de hacking*, 2018, 180; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 283.

[85] Destacan este cambio en la reforma de 2015, entre otros, CASTELLÓ NICÁS, en: MORILLAS CUEVA (dir.), *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, 2015, 506; ALMENAR PINEDA, *El delito de hacking*, 2018, 182; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 286-287.

La falta de autorización dota de relevancia penal a la conducta del delito de hacking, al entrar en el campo de la confidencialidad. Además, la existencia de medidas de seguridad, haciendo que el sistema esté protegido, hace evidente que el titular no quiere que se acceda al sistema de información[86].

Ejemplos de ello lo podemos encontrar en la SAP de Cáceres de 24 de julio de 2020[87], donde el denunciado realizó varios accesos no consentidos a la página web de la denunciante. O en la STC de 7 de noviembre de 2016[88], donde el denunciado accedió sin tener la autorización pertinente al correo electrónico del denunciante.

Tanto en el art. 1.d) de la Decisión Marco 2005/222/JAI, como en el art. 2 de la Directiva 2013/40/UE se define en términos similares "sin estar autorizado" como el acceso, interferencia o interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional[89].

La nueva redacción del art. 197 bis.1 CP exige una autorización debida. Entre las eximentes que pueden dar contenido a la justificación del hecho, porque se cuenta con la autorización debida, ha de mencionarse necesariamente el consentimiento otorgado por el titular del bien jurídico para que el sujeto activo acceda al sistema, o para que este sujeto activo facilite el acceso a un tercero. Este consentimiento puede ser tanto expreso como tácito, pero no debe quedar duda de su existencia, sin que la falta de oposición del titular pueda considerarse una autorización tácita para el acceso[90]. Habrá de aplicarse la teoría general sobre el consentimiento como eximente en DP para que surta los efectos de exclusión de la responsabilidad penal[91].

---

[86] Así lo matizan, ALMENAR PINEDA, *El delito de hacking*, 2018, 182; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 94; PALAZZI, en: DUPUY (dir.)/KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, 2018, 42.

[87] SAP Cáceres núm. 466/2020, de 24 de julio.

[88] STC núm. 319/2016, de 7 de noviembre.

[89] Para la interpretación de este requisito recurren a la normativa mencionada en el texto, entre otros, ALMENAR PINEDA, *El delito de hacking*, 2018, 183; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 288.

[90] Así lo aclara ALMENAR PINEDA, *El delito de hacking*, 2018, 184-185.

[91] Para más detalles, véase, entre otros, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 37; ALMENAR PINEDA, *El delito de hacking*, 2018, 184.

En la SAP Girona de 22 de septiembre de 2014[92], tenemos el caso en el que el sujeto ha sido absuelto porque no se consiguió probar esa falta de autorización necesaria para poder encontrarnos dentro del tipo.

La alusión del art. 197 bis.1 CP a estar debidamente autorizado puede plantear problemas sobre la legitimidad de la persona autorizante. Entre otros supuestos problemáticos se puede citar el supuesto referido a que el titular sea un menor de edad. Habrá que estar a lo dispuesto en la normativa que tiene incidencia directa en materia tecnológica para decidir si un menor de edad puede otorgar o no consentimiento válidamente[93]. Desde esta perspectiva, a partir de los catorce años, la capacidad del menor para otorgar un consentimiento eficaz y excluir la tipicidad va a depender del grado de madurez para la comprensión del alcance y trascendencia de dicha decisión, considerando el interés superior del menor y con carácter restrictivo[94].

Además de la autorización pertinente por parte del propietario del sistema o su titular legítimo, también cabe la posibilidad de que sea la autoridad judicial la que permita el acceso en los casos legalmente previstos[95]. En concreto, la autorización judicial para el acceso informático se encuentra en la LECrim en el Título VIII "De las medidas de investigación limitativas de los derechos reconocidos en el artículo 18 de la Constitución", dentro de este Título se encuentra el Capítulo IV "Disposiciones comunes a la interceptación de las comunicaciones telefónicas y telemáticas, la captación y grabación de comunicaciones orales mediante la utilización de dispositivos electrónicos, la utilización de dispositivos técnicos de seguimiento, localización y captación de imagen, el registro de dispositivos de almacenamiento masivo de información y los registros remotos sobre equipos informáticos"

[92] SAP Girona núm. 504/2014, de 22 de septiembre.
[93] En el art. 13 del Reglamento de la LOPD se establece que podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela, mientras que en el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
[94] Sobre este tema, véase, RUEDA MARTÍN, *Indret* 4 (2013), 32; ALMENAR PINEDA, *El delito de hacking*, 2018, 185-186.
[95] Sobre este otro supuesto de justificación, ALMENAR PINEDA, *El delito de hacking*, 2018, 187-188; BUJOSA VADELL, en: NAVAS GARCÉS (coord.), *Ciberdelitos*, 2019, 70-75.

donde se encuentran las denominadas pruebas tecnológicas que abarcan los arts. 588 bis a – 588 bis k LECrim[96].

Dentro del mismo Título VIII LECrim se encuentra el Capítulo VIII "Registro de dispositivos de almacenamiento masivo de información". En dicho Capítulo se establece la necesidad de la motivación individualizada cuando se produzca un registro domiciliario, debiendo extenderse la resolución judicial a los motivos que legitimen el acceso a la información contenida en los dispositivos. La simple incautación de los dispositivos durante un registro domiciliario no autoriza el acceso a su contenido, aunque posteriormente pueda ser autorizado judicialmente acorde al art. 588 sexies a) LECrim. En la autorización judicial que permite el acceso se determinarán las condiciones y alcance, incluyendo copias de datos y medidas para garantizar la integridad de los datos[97].

Dicha autorización judicial debe contar con los siguientes requisitos[98]:

- Especialidad: solo se puede autorizar la investigación tecnológica para delitos concretos.
- Idoneidad: se debe definir el ámbito objetivo y subjetivo de la medida, así como su duración.
- Excepcionalidad: solo se puede conceder esta autorización en el caso de que no existan medidas menos gravosas para los derechos fundamentales del investigado.
- Necesidad: solo se concede la autorización judicial cuando la investigación del delito se vea gravemente perjudicada.
- Proporcionalidad: se debe tener en cuenta la gravedad del hecho, su trascendencia social o la intensidad de los indicios existentes y la relevancia del resultado perseguido con la restricción del derecho.

[96] Para más detalles, véase ALMENAR PINEDA, *El delito de hacking*, 2018, 189; TEMPERINI, en: DUPUY (dir.)/KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, 2018, 241-243; BUJOSA VADELL, en: NAVAS GARCÉS (coord.), *Ciberdelitos*, 2019, 67.

[97] A pesar de esto, el art. 588 sexies c. 4 LECrim permite el acceso a los datos por parte de la Policía Judicial en casos de urgencia, es decir, no se tiene una autorización judicial previa. Así lo advierte también ALMENAR PINEDA, *El delito de hacking*, 2018, 190.

[98] VELASCO NÚÑEZ/SANCHIS CRESPO, *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, 2019, 272-289.

En el ámbito procesal rige el principio *in dubio pro reo*, es decir, el que acuse deberá acreditar que no existe la debida autorización, aunque también es suficiente el reconocimiento por parte del sujeto que haya realizado el acceso no consentido. En resumen, la falta de consentimiento no se puede presumir[99].

El criterio que tiene el TS en cuanto al acceso policial a un sistema informático es que no es suficiente la previa autorización judicial, también es necesario un razonamiento judicial para autorizar el sacrificio de los derechos que el acceso al sistema informático conlleva[100].

4. Objeto material

En cuanto al objeto material del delito de hacking, se debe hacer una diferenciación entre el objeto material tras la LO 5/2010 y el objeto material a partir de la reforma de la LO 1/2015.

El objeto material en el antiguo art. 197.3 CP reformado en 2010 lo constituía cualquier dato o programa informático, es decir, el objeto material de la acción serían los datos o programas informáticos que tenían que estar contenidos en un sistema informático o en parte del mismo[101].

La definición de "datos informáticos" la encontramos en el art. 2.b) de la Directiva 2013/40/UE que los define como toda representación de hechos, informaciones o conceptos de una forma que permite su tratamiento por un sistema de información, incluidos los programas que sirven para hacer que dicho sistema de información realice una función[102].

---

[99] ALMENAR PINEDA, *El delito de hacking*, 2018, 192.
[100] ALMENAR PINEDA, *El delito de hacking*, 2018, 189.
[101] MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 148; ALMENAR PINEDA, *El delito de hacking*, 2018, 140; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 257.
[102] MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 148; FERNÁNDEZ TERUELO, *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, 2011, 202; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 677; COLÁS TURÉGANO, *RBD* XXI (2016), 220; ALMENAR PINEDA, *El delito de hacking*, 2018, 140; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 176; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 256-257.

En cuanto a la definición de "programas informáticos", se debe acudir a la definición establecida en el art. 96.1 LPI: toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación[103].

El legislador con la reforma de la LO 1/2015 cambia el objeto material del delito, ya que ahora se refiere al conjunto o una parte de un sistema de información, mientras que antes se hacía referencia a los datos o programas informáticos contenidos en un sistema informático o en parte del mismo. Esto supone un adelantamiento de la barrera de protección del bien jurídico, pues ya no se exige el acceso a los datos o programas informáticos, sino que es suficiente con el acceso a todo o parte del sistema de información[104].

Esta modificación que afecta al objeto material se ha llevado a cabo para ajustarse a lo dispuesto en el art. 2.1 de la Decisión Marco 2005/222/JAI donde se establece que cada Estado miembro adoptará las medidas necesarias para que el acceso intencionado sin autorización al conjunto o a una parte de un sistema de información sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad. También resulta acorde con lo establecido en el art. 3 de la Directiva 2013/40/UE, donde también se pretende la tipificación penal del delito de intrusismo referido al acceso intencionado y sin autorización al conjunto o a una parte de un sistema de información, cuando tal acceso se haya cometido con violación de una medida de seguridad, al menos en los casos que no sean de menor gravedad[105].

La Directiva 2013/40/UE ofrece la siguiente definición de "sistema informático" en el art. 2.a): todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos

[103] Para más detalles sobre esta definición, entre otros, CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 253; MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 148; ALMENAR PINEDA, *El delito de hacking*, 2018, 140.

[104] Aluden a este adelantamiento en la protección del bien jurídico, COLÁS TURÉGANO, *RBD* XXI (2016), 220; ALMENAR PINEDA, *El delito de hacking*, 2018, 140-141; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 94; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 279.

[105] ALMENAR PINEDA, *El delito de hacking*, 2018, 141.

informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento[106].

El legislador no ha introducido en el CP la definición de sistema de información contenida en los instrumentos internacionales, como sí ha ocurrido en otros países como Chipre, Australia, Bulgaria o Rumanía. A falta de una definición propia, el término sistema informático ha de implementarse con la citada normativa comunitaria[107].

5. Tipo agravado por actuación en el seno de una organización o grupo criminal

El tipo agravado aparece descrito en el art. 197 quater CP que especifica que, si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.

Esta cualificación obedece a la gravedad derivada de la mayor capacidad delictiva de una organización dedicada a este tipo de actividades[108]. En un sentido similar, se ha señalado que el motivo de establecer un tipo agravado es para prevenir y mejorar la lucha contra la criminalidad organizada a través de las nuevas tecnologías, en este tipo de conductas existe un mayor desvalor de la acción debido a la facilidad que supone realizar estas conductas a través de una organización o grupo criminal[109].

---

[106] Sobre este concepto, véase, entre otros, MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 148; RUEDA MARTÍN, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, 2010, 360; COLÁS TURÉGANO, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 677; COLÁS TURÉGANO, *RBD* XXI (2016), 220; ALMENAR PINEDA, *El delito de hacking*, 2018, 143; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 176, 197; HERNÁNDEZ DÍAZ, *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, 2019, 279.

[107] ALMENAR PINEDA, *El delito de hacking*, 2018, 143.

[108] De esta opinión, SUÁREZ-MIRA RODRÍGUEZ/JUDEL PRIETO/PIÑOL RODRÍGUEZ, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 172.

[109] Propone esta explicación sobre el fundamento del tipo agravado ALMENAR PINEDA, *El delito de hacking*, 2018, 258.

Para la interpretación de los términos organización o grupo criminal hay que recurrir a los delitos tipificados en los arts. 570 bis y siguientes CP[110], preceptos penales que se han incorporado al texto punitivo en cumplimiento de varios compromisos internacionales[111], en particular, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, hecho en Nueva York el 15 de noviembre de 2000, donde se define la organización criminal como un grupo criminal organizado, esto es, un grupo estructurado de tres o más personas que existe durante un cierto tiempo y que actúa concertadamente con el propósito de cometer uno o más delitos graves, con la intención de obtener, directa o indirectamente un beneficio material o económico[112].

También la previsión de esta circunstancia cualificante en el delito de intrusismo informático es consecuencia de la adaptación del Derecho interno a lo dispuesto en la normativa europea sobre delincuencia cibernética, concretamente, a lo dispuesto en el art. 7.1 de la DM 2005/222/JAI y en el Considerando 13 de la Directiva 2013/40/UE, donde se justifica tal previsión porque resulta conveniente establecer sanciones más severas cuando un ataque contra un sistema de información se comete en el contexto de una organización delictiva[113].

Como se ha indicado, en el art. 570 bis CP se ha tipificado el delito de organización criminal, que se define como la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos[114].

---

[110] ALMENAR PINEDA, *El delito de hacking*, 2018, 258; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 182.

[111] Recurren a este argumento, entre otros, GARCÍA RIVAS/LAMARCA PÉREZ, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 504; ALMENAR PINEDA, *El delito de hacking*, 2018, 258-260.

[112] Sobre este concepto, véase FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 94.

[113] ALMENAR PINEDA, *El delito de hacking*, 2018, 258.

[114] La definición de organización criminal ha de ser tomada en consideración para interpretar el tipo cualificado que nos ocupa. Véase, para más detalles, CARRASCO ANDRINO, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 255; GARCÍA RIVAS/LAMARCA PÉREZ, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 507; MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 155; FERNÁNDEZ HERNÁNDEZ, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 1348; ALMENAR PINEDA, *El delito de hacking*, 2018, 265; FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 96-97.

Por tanto, la criminalidad organizada puede definirse como la manifestación de la participación criminal en el delito con fórmulas de concertación delictiva que superan la mera individualidad. Con Internet y las nuevas tecnologías se han visto favorecidos, ya que es necesario tener al grupo en contacto constantemente, pueden atacar bienes jurídicos a través de las nuevas tecnologías o incluso llegar a dañar o destruirlas[115].

Es decir, para que exista una organización criminal son necesarias más de dos personas y la actuación de forma concertada, por tiempo indefinido y todo ello con el fin de cometer delitos[116].

Por otro lado, en el art. 570 ter CP se ofrece la definición de grupo criminal, que consiste en la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal, tenga por finalidad o por objeto la perpetración concertada de delitos[117].

En la STS de 22 de diciembre de 2014[118] se resalta el elemento distintivo entre una organización y un grupo criminal, ya que en una organización criminal se encuentra el carácter estable y la concertación y coordinación en el reparto de funciones; estos son los elementos o características que han de faltar en el grupo criminal.

A pesar de que se ha destacado la utilidad de la agravante en el delito de hacking, no se entiende que se haya decidido equiparar a efectos de pena entre el hecho cometido por una organización y el cometido por un grupo criminal, pues los delitos con este *nomen iuris* no reciben un tratamiento punitivo idéntico[119].

---

[115] ALMENAR PINEDA, *El delito de hacking*, 2018, 257-258.

[116] FERNÁNDEZ HERNÁNDEZ, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 1348; ALMENAR PINEDA, *El delito de hacking*, 2018, 266.

[117] Sobre el concepto de grupo criminal, véase, entre otros, GARCÍA RIVAS/LAMARCA PÉREZ, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, 2010, 508; MIRÓ LLINARES, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 155; FERNÁNDEZ HERNÁNDEZ, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 1349; ALMENAR PINEDA, *El delito de hacking*, 2018, 267; FERNÁNDEZ BERMEJO/MARTÍNEZ ATIENZA, *Ciberseguridad, ciberespacio y ciberdelincuencia*, 2018, 101.

[118] STS núm. 877/2014, de 22 de diciembre.

[119] De esta opinión, entre otros, ALMENAR PINEDA, *El delito de hacking*, 2018, 271.

III. LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

Como ya se ha señalado anteriormente, la responsabilidad penal de las personas jurídicas está prevista en el art. 197 quinquies CP.

Como ya es conocido, desde la reforma operada por la LO 5/2010 se ha establecido la responsabilidad penal de las personas jurídicos en el ordenamiento español. Esta responsabilidad penal no se amplía, esto es, no abarca todas las figuras delictivas tipificadas en el CP, sino que se ha limitado a un número cerrado de hechos delictivos. Entre los tipos penales que pueden dar lugar a responsabilidad penal de las personas jurídicas se cuenta el delito de intrusismo informático, ya desde la reforma de 2010, y se confirma nuevamente en la reforma de 2015.

En la reforma de 2010 el legislador español ha previsto esta responsabilidad en cumplimiento con las exigencias fijadas en la Decisión Marco 2005/222/JAI, si bien hay que señalar que, realmente, este texto europeo no exigía que la responsabilidad de las personas jurídicas tuviera que tener necesariamente naturaleza penal[120]. La reforma de 2015 ha tratado de adaptar la regulación penal del delito de intrusismo a lo dispuesto en la Directiva 2013/40/UE, donde se prevé una disposición para la fijación de la responsabilidad de las personas jurídicas, pero nuevamente no se establece que dicha responsabilidad haya de tener naturaleza penal[121].

1. Criterios para imputar la responsabilidad penal de la persona jurídica

Para imputar la responsabilidad penal a la persona jurídica por la comisión de un delito de intrusismo informático ha de cumplirse lo dispuesto en el art. 31 bis CP. Este precepto penal establece dos criterios de imputación de responsabilidad penal a la persona jurídica[122]:

---

[120] Así lo han advertido, entre otros, GONZÁLEZ COLLANTES, *RDPC* 13 (2015), 78; ALMENAR PINEDA, *El delito de hacking*, 2018, 297.

[121] Insiste en esta idea, ALMENAR PINEDA, *El delito de hacking*, 2018, 297-298.

[122] Sobre el art. 31 bis CP, véase, entre otros muchos, DOPICO GÓMEZ-ALLER, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, 2010, 16-20; MORILLAS CUEVA, *Anales de Derecho* 29 (2011), 23; GONZÁLEZ CUSSAC, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 164-178; ALMENAR PINEDA, *El delito de hacking*, 2018, 298-299; PORRES ORTIZ DE

a) De los delitos cometidos en nombre o por cuenta de las mismas, y en su beneficio directo o indirecto, por sus representantes legales o por aquellos que actuando individualmente o como integrantes de un órgano de la persona jurídica, están autorizados para tomar decisiones en nombre de la persona jurídica u ostentan facultades de organización y control dentro de la misma.

b) De los delitos cometidos, en el ejercicio de actividades sociales y por cuenta y en beneficio directo o indirecto de las mismas, por quienes, estando sometidos a la autoridad de las personas físicas mencionadas en el párrafo anterior, han podido realizar los hechos por haberse incumplido gravemente por aquéllos los deberes de supervisión, vigilancia y control de su actividad atendidas las concretas circunstancias del caso.

Con esta previsión se trata de incentivar que las personas jurídicas asuman una autoorganización para impedir que se cometan delitos en su seno con el fin de lograr sus objetivos sociales, de tal manera que sea la persona jurídica quien adopte medidas para investigar y evitar conductas que, aunque sean delictivas, le puedan favorecer. La estructura compleja de las empresas dificulta la investigación de los delitos cometidos en su seno o puede facilitar que se desplace la responsabilidad a niveles inferiores, por ello aparte de imponer una pena, también se obliga a las sociedades a tener determinadas medidas a modo de prevención, una exigencia que se ha previsto expresamente como eximente de la responsabilidad penal de las personas jurídicas en la reforma de 2015[123].

El legislador español no ha incluido un concepto positivo de persona jurídica en el CP, por lo que se debe seguir la definición que ofrecen los instrumentos internacionales[124].

El art. 1 de la Decisión Marco 2005/222/JAI y el art. 2 de la Directiva 2013/40/UE definen a la persona jurídica de manera similar: toda entidad en la cual el derecho vigente reconoce este estatuto, salvo los Estados y otros organismos públicos que ejercen prerrogativas estatales y las organizaciones internacionales de derecho público. La Directiva 2013/40/UE

URBINA, *Responsabilidad penal de las personas jurídicas*, en https://elderecho.com/responsabilidad-penal-de-las-personas-juridicas-tribuna (consultado en fecha 17 de octubre de 2020).

[123] GONZÁLEZ CUSSAC, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 181; ALMENAR PINEDA, *El delito de hacking*, 2018, 299.

[124] Defienden esta tesis, entre otros, MORILLAS CUEVA, *Anales de Derecho* 29 (2011), 24-25; DE LA CUESTA ARZAMENDI, *RPM* 5 (2013), 25; ALMENAR PINEDA, *El delito de hacking*, 2018, 301.

cambia el término "prerrogativas estatales" por "prerrogativas públicas", esto es importante para nuestro ordenamiento interno, ya que pueden existir prerrogativas dimanantes de CCAA o entidades locales y ser igualmente públicas[125].

En el art. 31 quinquies CP sí se cuenta con una definición negativa de persona jurídica, es decir, se hace una enumeración de supuestos que quedan excluidos de la responsabilidad penal[126]:

- Las entidades de Derecho público, más concretamente, Estado, Administraciones públicas territoriales e institucionales, Organismos reguladores y organizaciones internacionales de derecho público.
- Las entidades públicas empresariales y privadas que ejercen funciones públicas, siendo estas, Agencias y Entidades públicas Empresariales y organizaciones que ejerzan potestades públicas de soberanía o administrativas.

Podemos entender como "persona jurídica a efectos del delito de hacking" a toda entidad a la cual el derecho vigente reconoce este estatuto, salvo el Estado, otros organismos públicos que ejercen prerrogativas públicas, las organizaciones internacionales de Derecho público, las Administraciones públicas territoriales e institucionales, los Organismos Reguladores, las Agencias y Entidades públicas Empresariales y las organizaciones que ejerzan potestades públicas de soberanía o administrativas. Para que todas estas entidades sean responsables del delito de hacking es necesario que una persona física lleve a cabo la conducta del art. 197 bis.1 CP y esta persona física, que actúa en nombre y en beneficio de la persona jurídica, tiene que ser el representante o tiene que ser una persona que esté sujeta a la autoridad de este[127].

Para entender que una persona jurídica ha cometido un delito de hacking deben concurrir dos requisitos dados por el TS en la STS de 29 de febrero de 2016[128]:

---

[125] Sobre este tema, véase, ALMENAR PINEDA, *El delito de hacking*, 2018, 302.

[126] Para más detalles sobre la interpretación de este precepto, entre otros, MORILLAS CUEVA, *Anales de Derecho* 29 (2011), 25; RODRÍGUEZ GARCÍA, *Los Retos del Poder Judicial ante la sociedad globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional)*, 2012, 206; DE LA CUESTA ARZAMENDI, *RPM* 5 (2013), 26; GONZÁLEZ CUSSAC, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 205; ALMENAR PINEDA, *El delito de hacking*, 2018, 302.

[127] ALMENAR PINEDA, *El delito de hacking*, 2018, 307-308.

[128] STS núm. 154/2016, de 29 de febrero.

- La comisión de uno de los delitos integrantes del catálogo de aquellas infracciones susceptibles de generar responsabilidad penal para la persona jurídica en cuyo seno se comete. Esta circunstancia se cumple con el citado art. 197 quinquies CP.
- Que las personas físicas autoras de dicho delito sean integrantes de la persona jurídica. En el intrusismo informático es necesario que sea llevado a cabo en beneficio de la persona jurídica.

El legislador español ha regulado la responsabilidad penal de la persona jurídica incluso no siendo posible individualizar a la persona física que ha cometido el delito de intrusismo informático[129]. Está previsto en el art. 31 ter CP:

1. La responsabilidad penal de las personas jurídicas será exigible siempre que se constate la comisión de un delito que haya tenido que cometerse por quien ostente los cargos o funciones aludidas en el artículo anterior, aun cuando la concreta persona física responsable no haya sido individualizada o no haya sido posible dirigir el procedimiento contra ella. Cuando como consecuencia de los mismos hechos se impusiere a ambas la pena de multa, los jueces o tribunales modularán las respectivas cuantías, de modo que la suma resultante no sea desproporcionada en relación con la gravedad de aquéllos.
2. La concurrencia, en las personas que materialmente hayan realizado los hechos o en las que los hubiesen hecho posibles por no haber ejercido el debido control, de circunstancias que afecten a la culpabilidad del acusado o agraven su responsabilidad, o el hecho de que dichas personas hayan fallecido o se hubieren sustraído a la acción de la justicia, no excluirá ni modificará la responsabilidad penal de las personas jurídicas, sin perjuicio de lo que se dispone en el artículo siguiente.

De esta previsión se deduce, además, que la responsabilidad penal de la persona jurídica no depende de la responsabilidad penal de la persona física, si bien sí debe existir un hecho de conexión que se atribuya a la persona física[130].

[129] Sobre la previsión del art. 31 ter CP, véase, entre otros, GONZÁLEZ CUSSAC, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 204-205; ALMENAR PINEDA, *El delito de hacking*, 2018, 314-315.
[130] De esta opinión, entre otros, BACIGALUPO SAGGESE, *LL* 7541 (2011); ALMENAR PINEDA, *El delito de hacking*, 2018, 314.

2. Medidas que la persona jurídica puede aplicar para quedar exento de responsabilidad

El art. 31 bis. 2 y 5 CP establece las medidas de contención y prevención que puede utilizar la persona jurídica para estar exenta de responsabilidad siempre que se cumplan las siguientes condiciones[131]:

- Que el órgano de administración haya adoptado y ejecutado con eficacia, antes de la comisión del delito, modelos de organización y gestión que incluyen las medidas de vigilancia y control idóneas para prevenir delitos de la misma naturaleza o para reducir de forma significativa el riesgo de su comisión.

  En el art. 31 bis. 5 CP se establecen que esos modelos de organización mencionados anteriormente, que deben cumplir una serie de requisitos:

  1.º Identificarán las actividades en cuyo ámbito puedan ser cometidos los delitos que deben ser prevenidos.

  2.º Establecerán los protocolos o procedimientos que concreten el proceso de formación de la voluntad de la persona jurídica, de adopción de decisiones y de ejecución de las mismas con relación a aquéllos.

  3.º Dispondrán de modelos de gestión de los recursos financieros adecuados para impedir la comisión de los delitos que deben ser prevenidos.

  4.º Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención.

  5.º Establecerán un sistema disciplinario que sancione adecuadamente el incumplimiento de las medidas que establezca el modelo.

  6.º Realizarán una verificación periódica del modelo y de su eventual modificación cuando se pongan de manifiesto infracciones relevantes de sus

[131] Véase, más ampliamente, GONZÁLEZ CUSSAC, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, 2015, 182-203; ALMENAR PINEDA, *El delito de hacking*, 2018, 315-317.

disposiciones, o cuando se produzcan cambios en la organización, en la estructura de control o en la actividad desarrollada que los hagan necesarios.

- Que la supervisión del funcionamiento y del cumplimiento del modelo de prevención implantado haya sido confiada a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica. En el art. 31 bis. 3 CP encontramos una especificación solo para las personas jurídicas de pequeñas dimensiones, es ese caso las funciones de supervisión a que se refiere la condición 2ª del apartado 2 podrán ser asumidas directamente por el órgano de administración. A estos efectos, son personas jurídicas de pequeñas dimensiones aquéllas que, según la legislación aplicable, estén autorizadas a presentar cuenta de pérdidas y ganancias abreviada.
- Pero además de los modelos y controles citados en los anteriores párrafos, los autores individuales deben cometer el delito eludiendo fraudulentamente los modelos de organización y de prevención.
- En relación con las medidas de prevención y control y la vulneración de los modelos, se exige a la persona jurídica un control mayor, es decir, no se debe producir una omisión o un ejercicio insuficiente de las funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición segunda, es decir, se refiere a un órgano de la persona jurídica con poderes autónomos de iniciativa y de control o que tenga encomendada legalmente la función de supervisar la eficacia de los controles internos de la persona jurídica. El legislador en este punto podría haber hecho una mayor concreción.
- El art. 31 bis. 2 CP finaliza con una especificación para los casos en los que las anteriores circunstancias solo puedan ser objeto de una acreditación parcial, dicha circunstancia será valorada a los efectos de atenuación de la pena.

Para la FGE estamos ante un supuesto de exclusión personal de punibilidad. En el momento en que la persona física comete el delito y transfiere la responsabilidad a la persona jurídica,

los modelos de organización que cumplen los presupuestos legales operarán a modo de excusa absolutoria, como una causa de exclusión personal de la punibilidad[132].

El TS en la STS de 29 de febrero de 2016 ha mantenido un criterio distinto a la FGE considerando que la eximente tiene una naturaleza que se correspondería con la falta de tipicidad. La exoneración se basa en la prueba de la existencia de herramientas de control idóneas y eficaces cuya ausencia integraría el núcleo típico de la responsabilidad penal de la persona jurídica, complementario de la comisión del ilícito por la persona física. En resumen, la existencia de las medidas de control y prevención evidenciarían la falta de responsabilidad de la entidad en el acceso ilícito a un sistema informático, evitando un juicio *ab initio* a la persona jurídica, cuando ha sido uno de sus empleados el que ha cometido el delito de intrusismo informático[133].

IV. LA RESPONSABILIDAD PENAL DEL FUNCIONARIO PÚBLICO

Como se ha explicado en el punto relativo al sujeto activo, el delito de intrusismo informático es un delito común, esto es, puede ser cometido por cualquier persona.

Para el caso de que esta persona sea una autoridad o funcionario público, sin embargo, ha de ser aplicado el tipo penal previsto en el art. 198 CP, o al menos a esta conclusión ha de llegarse, tal como se tratará de explicar en este apartado.

El art. 198 CP dispone lo siguiente: la autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

El art. 198 CP es un delito especial impropio debido a que las características del sujeto activo determinan un castigo diferente. Se trata de un tipo cualificado por razón del sujeto activo,

[132] ALMENAR PINEDA, *El delito de hacking*, 2017, 665-666.
[133] STS núm. 154/2016, de 29 de febrero. Sobre la crítica a esta interpretación del TS, ALMENAR PINEDA, *El delito de hacking*, 2018, 320.

teniendo un doble fundamento, la mayor facilidad para cometer el delito y la vulneración de su deber de corrección en el cumplimiento de su cargo[134].

Un ejemplo de ello, lo encontramos en la STS de 8 de octubre de 2020[135] donde un funcionario de la Policía Nacional empleó la contraseña de un compañero que había obtenido por su condición de funcionario público con una finalidad diferente a la prevista legalmente. También en la STS de 23 de abril de 2019[136] en la que un funcionario del Servicio de Vigilancia Aduanera de la Agencia Estatal Tributaria, abusando de su condición y de la autorización que tenía, consultó las bases de datos de dicho organismo en relación a la investigación del posible blanqueo en materia de importaciones y exportaciones aduaneras. O la SAP Valencia de 4 de mayo de 2012[137], en la que un Guardia Civil utilizó su tarjeta y claves para consultar la terminal informática oficial de la Guardia Civil, realizando búsquedas de datos personales que nada tenían que ver con su cargo.

Aunque también encontramos casos en los que a pesar de que el denunciado tenga un cargo público no se aprovecha de ello para conseguir el acceso a la información, como es el caso de la SAP Sevilla de 7 de diciembre de 2011[138], donde la denunciada que trabajaba en un hospital consiguió una historia clínica sin usar las ventajas que tenía como administrativa del hospital.

1. Los requisitos del art. 198 CP

En el art. 24 CP tenemos la definición de autoridad y de funcionario público. Este precepto define como "autoridad", al que por sí solo o como miembro de alguna corporación, tribunal u órgano colegiado tenga mando o ejerza jurisdicción propia. En todo caso, tendrán la consideración de autoridad los miembros del Congreso de los Diputados, del Senado, de las

[134] De esta opinión, entre otros, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 46-47; RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 122-123; SUÁREZ-MIRA RODRÍGUEZ/JUDEL PRIETO/PIÑOL RODRÍGUEZ, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, 2012, 173; ALMENAR PINEDA, *El delito de hacking*, 2018, 278-279, 288-288.
[135] STS núm. 494/2020, de 8 de octubre.
[136] STS núm. 211/2019, de 23 de abril.
[137] SAP Valencia núm. 335/2012, de 4 de mayo.
[138] SAP Sevilla núm. 76/2011, de 7 de diciembre.

Asambleas Legislativas de las Comunidades Autónomas y del Parlamento Europeo. Se reputará también autoridad a los funcionarios del Ministerio Fiscal. Mientras que "funcionario público" sería todo el que por disposición inmediata de la Ley o por elección o por nombramiento de autoridad competente participe en el ejercicio de funciones públicas[139].

Para la aplicación de este tipo penal cualificado se ha establecido como requisito típico que la conducta sea llevada a cabo fuera de los casos permitidos por la Ley. La autoridad o funcionario público obra fuera de sus competencias, como si fuera un particular, pero con prevalimiento de la condición especial que posee, siendo evidente que actúa fuera de la ley y fuera de sus competencias[140].

Al igual que en el art. 197 bis.1 CP, también aquí es necesaria la falta de autorización, independientemente de la condición de autoridad o funcionario público[141].

Otro de los elementos típicos de esta figura agravada es que la autoridad o funcionario público ha de actuar sin mediar causa legal por delito. La causa por delito existe cuando, constando un hecho delictivo que esté al menos racionalmente indiciado y que sea imputable a una o varias personas, se produce una actuación policial o judicial dirigida a la averiguación de ese hecho o al aseguramiento de la persona o personas presuntamente responsables. La existencia de un procedimiento judicial o diligencias policiales sería lo que determinase si media causa por delito, y, por tanto, si entra o no dentro de lo establecido en el art. 198 CP[142].

La autoridad o funcionario ha de actuar prevaliéndose de su cargo; esto quiere decir que el sujeto debe aprovecharse de la función que realiza para cometer la conducta delictiva con

---

[139] Sobre la interpretación de este precepto, véase, entre otros, ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 47; RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 121-122; ALMENAR PINEDA, *El delito de hacking*, 2018, 279.
[140] ORTS BERENGUER/ROIG TORRES, *Delitos informáticos y delitos comunes cometidos a través de la informática*, 2001, 47; RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 123; ALMENAR PINEDA, *El delito de hacking*, 2018, 281; SIERRA LÓPEZ, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, 2018, 183.
[141] ALMENAR PINEDA, *El delito de hacking*, 2018, 283.
[142] RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 127-128; ALMENAR PINEDA, *El delito de hacking*, 2018, 285-286.

mayor facilidad[143]. En definitiva, se trata de la misma interpretación que ha de mantenerse para la agravante genérica contenida en el art. 22.7ª CP, consistente en prevalerse del cargo público que tenga el culpable. Obviamente, esta circunstancia agravante genérica no es aplicable al art. 198 CP al ser inherente al mismo[144].

El aspecto que resulta más problemático es que el art. 198 CP, para la descripción de las conductas típicas, hace una remisión al artículo anterior. Pero el artículo inmediatamente anterior está regulando la responsabilidad penal de las personas jurídicas en relación con los delitos descritos en el Capítulo. Ha de entenderse que, en realidad, la remisión también va referida a los delitos tipificados en el Capítulo, pero en la reforma de 2015, cuando se introducen los arts. 197 bis a 197 quinques, el legislador olvidó revisar la redacción de este tipo cualificado.

En resumen, el art. 198 CP supone un abuso de las facultades obtenidas con la condición de autoridad o funcionario público para poder llevar a cabo un acceso ilícito, facilitarlo o mantenerse en un sistema informático. Al hacerlo, el sujeto infringe el deber de conservar la integridad y seguridad de los sistemas de información, además accede a todo o parte del sistema de manera ilegal gracias a su posición de autoridad o funcionario público, por lo que se justifica una mayor pena para estos casos[145].

2. El art. 198 CP y los problemas concursales con otros delitos

Por último, cabe señalar que el art. 198 CP plantea problemas concursales con otros delitos, en particular, con los tipificados en los arts. 414, 415 y 536 CP:

El art. 414 CP se compone de dos párrafos, a la autoridad o funcionario público que, por razón de su cargo, tenga encomendada la custodia de documentos respecto de los que la autoridad competente haya restringido el acceso, y que a sabiendas destruya o inutilice los

[143] RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 123; ALMENAR PINEDA, *El delito de hacking*, 2018, 286.
[144] RUEDA MARTÍN, *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, 2004, 123; ALMENAR PINEDA, *El delito de hacking*, 2018, 287.
[145] Sobre este tema, véase, ALMENAR PINEDA, *El delito de hacking*, 2018, 288.

medios puestos para impedir ese acceso o consienta su destrucción o inutilización, incurrirá en la pena de prisión de seis meses a un año o multa de seis a veinticuatro meses y, en cualquier caso, inhabilitación especial para empleo o cargo público por tiempo de uno a tres años. Y, en el segundo párrafo, el particular que destruyere o inutilizare los medios a que se refiere el apartado anterior, será castigado con la pena de multa de seis a dieciocho meses. Se trata del acceso a documentos y no necesariamente a un sistema informático en el que se pudieran encontrar. En el caso de darse esta conducta junto con la de intrusismo informático, se tendría que resolver con un concurso de normas entre ambos artículos.

El art. 415 CP establece que, la autoridad o funcionario público no comprendido en el artículo anterior que, a sabiendas y sin la debida autorización, accediere o permitiere acceder a documentos secretos cuya custodia le esté confiada por razón de su cargo, incurrirá en la pena de multa de seis a doce meses, e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años. En este caso, se podría plantear que esos documentos secretos se encontraran en un sistema informático. Al igual que en el caso anterior, en el supuesto de darse ambas conductas se aplicaría un concurso de normas entre ambos artículos.

El art. 536 CP dispone que la autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escucha, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años. Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses. El art. 198 CP exige que además de acceder al sistema informático, la autoridad o funcionario público actúe fuera de los casos permitidos por Ley, sin mediar causa legal por el delito y prevaliéndose de su cargo. Es decir, incluye conductas en el ámbito de las relaciones de la Administración-ciudadano y otras relaciones Estado-ciudadano, cuando no medie la investigación de una causa penal. Por lo que se podría plantear un concurso de leyes entre ambos artículos si se dan ambas conductas. Aunque también se ha mantenido la postura de que el art. 536 CP configura un supuesto de tipicidad bien delimitado en relación con los elementos típicos del art. 198 CP, por lo que no parece que pudiera plantearse un concurso de normas. Podría ocurrir que la autoridad o funcionario público intercepte las telecomunicaciones o utilice algunos de los

artificios que menciona el art. 536 CP para acceder al sistema informático, en estos casos se tendría que analizar la concurrencia de las circunstancias que integran el tipo del art. 536 y 198 CP para ver cuál de los dos podría aplicarse[146].

V. PERSEGUIBILIDAD

Uno de los principales obstáculos que podemos encontrar en la lucha contra la ciberdelincuencia son los factores técnicos que dificultan la detección y persecución del delito que se comete a través de Internet[147]. Esto explica el gran éxito que tiene este medio como canal de ejecución delictiva. Dos de los grandes factores facilitadores de su comisión son el anonimato del autor y la ejecución del delito a distancia[148].

Las dificultades existentes para esclarecer la comisión de un delito ejecutado a través de Internet pueden ser significativas, pero esto no quiere decir que aquel deba quedar impune, sino que se deben intensificar los esfuerzos para lograr medios adecuados de investigación y persecución[149].

Es cierto que se han creado nuevas secciones especializadas en delincuencia informática en los cuerpos policiales para facilitar la labor de seguimiento de los delitos, pero ocurre a veces que es el propio perjudicado el que no denuncia el hecho, al no considerarlo importante y otras veces es la propia autoridad la que no ve importante el hecho[150]. De ahí la importancia de denunciar el delito, ya que de acuerdo con la previsión contemplada en el art. 201 CP,

---

[146] Sobre los problemas concursales descritos en el texto, véase ALMENAR PINEDA, *El delito de hacking*, 2018, 275-277.

[147] Véase, entre otros muchos, MATELLANES RODRÍGUEZ, *RICPC* XXVI (2005), 134; FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 14; DÍEZ GÓMEZ, *REDUR* 8 (2010), 173; ASENCIO GALLEGO, en: ASENCIO MELLADO (dir.)/FERNÁNDEZ LÓPEZ (coord.), *Justicia penal y nuevas formas de delincuencia*, 2017, 45.

[148] Véase, por todos, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 14; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 43.

[149] Reclamaban este esfuerzo, entre otros, MATELLANES RODRÍGUEZ, *RICPC* XXVI (2005), 134; DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 89.

[150] DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 20; PÉREZ ESTRADA, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 307.

para poder proceder por los delitos de intrusismo informático será necesaria la denuncia de la persona afectada o de su representante legal[151].

1. El anonimato del autor

La tarea de delimitar quien es el autor del hecho delictivo no es siempre sencilla. Cada dispositivo conectado a Internet tiene asignado una dirección IP, tendría los mismos efectos que un DNI electrónico. Su detección y seguimiento en muchos casos no resulta complejo ya que es un dato público y de carácter personal. El problema es que se han desarrollado técnicas que sirven para ocultar o manipular dicha dirección, como el conectarse a redes wi-fi abiertas, utilización de proxies o VPNs o incluso la creación de redes botnet[152].

Una vez determinada la dirección IP, el proceso para identificar al titular de la línea se inicia mediante solicitud al juzgado para que autorice mandamiento dirigido a los proveedores de acceso a Internet y operadores de telecomunicaciones que asignaron a la misma, con el fin de que informen de los datos que posean para proceder a la identificación[153].

A continuación, mediante auto del juzgado que lo autoriza, se lleva a cabo la diligencia de entrada y registro en el domicilio o sede del titular de la línea, en cuya acta levantada por el

[151] COLÁS TURÉGANO, *RBD* XXI (2016), 226.

[152] Se debe hacer una mención especial a la red Tor, un proyecto cuyo principal objetivo es el desarrollo de una red de comunicaciones superpuesta sobre Internet que permite ocultar la identidad de los usuarios al no revelar su dirección IP, además mantiene el secreto y la integridad de la información al encriptar su tráfico por capas, como si fuera una cebolla. Debido a esta peculiaridad se dice que esta red pertenece a la red oscura o darknet. Es importante destacar que la red Tor no está desarrollada para favorecer la criminalidad en Internet, su principal objetivo es poder navegar por el ciberespacio de forma segura y anónima, lejos del control de gobiernos y grandes empresas de Internet. A pesar de que no fue diseñada para ello, la red Tor posee un porcentaje significativo de contenidos ilegales, como venta de armas y drogas o pornografía infantil. Para más detalles, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 14; DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 91-92; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 44.

[153] FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 14; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 44-45; TEMPERINI, en: DUPUY (dir.)/KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, 2018, 231.

LAJ se hace constar que se accede al ordenador y a los ficheros del sujeto, obteniendo una copia de los mismos[154].

Al principio de la era de Internet, la identificación de la máquina desde la que se ejecutaba la conducta delictiva era especialmente difícil por las escasas obligaciones de control impuestas a los proveedores de Internet y operadores de telecomunicaciones, además de no tener los archivos log, un instrumento técnico donde se recogen las asignaciones de las direcciones IP de los usuarios físicos[155].

En un primer momento, la LSSI reforzó las posibilidades de identificación de comportamientos que pueden tener un carácter delictivo. Se estableció la obligación para determinados proveedores de servicios de Internet de realizar una serie de actuaciones que pudieran servir a los órganos judiciales y policiales en la investigación de delitos cometidos a través de Internet[156].

La LCDCE derogó las previsiones introducidas por la LSSI. Esta Ley es la transposición interna de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones y por la que se modifica la Directiva 2002/58/CE, cuyo objetivo es establecer, a nivel europeo, la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por éstos con el fin de hacer posible que dispongan de ellos los agentes facultados. Esta nueva Ley pretende hacer frente a las dificultades de persecución de las nuevas formas delictivas a través de Internet, ya que para

[154] FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 14; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 45.

[155] FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 15; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 45.

[156] Véase, más ampliamente, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 15; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 45.

delimitar quién es el presunto autor es necesaria la localización del dispositivo desde el que se ejecuta la acción y el contenido de las comunicaciones[157].

La LCDCE instituye la obligación de los operadores de telecomunicaciones de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas, además del deber de cesión de dichos datos a los agentes facultados, siempre y cuando sean requeridos a través de una autorización judicial. De esta misma Ley deben destacarse los arts. 1, 3 y 4. En el art. 1 LCDEC se dispone que la ley se aplica a los datos de tráfico y localización sobre personas físicas y jurídicas y a los datos necesarios para identificar al abonado o usuario registrado, incluida la información que se consulta usando una red de comunicaciones electrónicas. El art. 3 LCDEC establece los datos objeto de conservación, mientras que en el art. 4 LCDEC se fija un plazo de conservación de doce meses, computados desde la fecha en que se haya producido la comunicación[158].

Pero, aun consiguiendo determinar el terminal desde el que se ha ejecutado la conducta delictiva, las dificultades para identificar al autor pueden persistir. Puede que el equipo usado se encuentre en un lugar público, como una universidad, o que haya utilizado conexiones wi-fi ajenas mediante su pirateo. Por ello es necesario que tanto las personas físicas como jurídicas adopten medidas de seguridad para proteger sus sistemas[159].

[157] Sobre este tema, véase, DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 92-93; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 46.

[158] BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 46-47.

[159] FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 19; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 50.

2. La ejecución del delito a distancia

El segundo gran problema en cuanto a la persecución del delito es cuando se comete a distancia, lo que presenta dificultades a la hora de determinar el lugar de comisión del delito y, por tanto, la competencia territorial para juzgar los hechos[160].

La conducta delictiva puede iniciarse en uno o varios países y causar efectos en otro u otros. Puede resultar difícil precisar donde tiene lugar la acción ya que la conducta delictiva navega por el ciberespacio. Esto plantea serios problemas a la hora de determinar la competencia jurisdiccional para su enjuiciamiento, ya que la regla general en materia de competencia es el lugar de la comisión del delito, aplicando el principio de territorialidad del art. 23.1 LOPJ[161].

Lo que dificulta, además, la persecución en este caso es que el material ilícito puede ser rápidamente trasladado a otro servidor o plataforma. Debido al carácter internacional de Internet, los sujetos alojan las páginas web con contenidos ilícitos en servidores de otros países donde la legislación es menos restrictiva, por ejemplo, donde tales contenidos se consideran legales. La principal consecuencia de esto es que, al iniciarse una investigación en el país afectado, el contenido ilícito puede encontrarse fuera de la jurisdicción penal[162].

La solución puede encontrarse precisando en qué lugar se entiende cometido el delito. Existen tres construcciones jurídicas que ofrecen soluciones a este problema[163]:

---

[160] DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 20; DÍEZ GÓMEZ, *REDUR* 8 (2010), 175; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 50.

[161] FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 20; DE LA CUESTA ARZAMENDI/PÉREZ MACHÍO/SAN JUAN GUILLÉN, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 95; DE LA MATA BARRANCO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, 2010, 26-27; PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 247; RAYÓN BALLESTEROS/GÓMEZ HERNÁNDEZ, *AJEE* 47 (2014), 215; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 50.

[162] PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 248; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 51.

[163] Sobre estas teorías, entre otros muchos, FERNÁNDEZ TERUELO, *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, 2007, 21; PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010,

- Teoría de la actividad: el delito se entiende cometido donde el sujeto lleva a cabo externamente la conducta delictiva.
- Teoría del resultado: el delito se perpetra donde tiene lugar el resultado externo. Se refiere a la interpretación física de lo que es el resultado del delito.
- Teoría de la ubicuidad: el delito se entiende cometido donde se lleva a cabo la actividad o se manifiesta el resultado. De esta manera la jurisdicción nacional entraría en juego tanto si la acción se llevó a cabo en su territorio y el resultado tuvo lugar fuera, como si el hecho se realizó fuera y el resultado se produjo en su territorio.

La teoría de la ubicuidad parece ser la más aceptada, pues favorece la posibilidad de que el hecho delictivo no quede impune por falta de competencia para la persecución penal. Como contrapartida, con esta teoría pueden declararse competentes varios Estados para la persecución del hecho delictivo, tantos como se hayan visto afectados por la acción o el resultado del delito; en estos casos habrá que atender a la normativa en materia de cooperación internacional para que, finalmente, solo uno de los Estados conozca del hecho delictivo y el resto cooperen con él en el esclarecimiento de los hechos[164].

249-252; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 51.

[164] PÉREZ MACHÍO, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), Derecho *penal informático*, 2010, 250-251; BARRIO ANDRÉS, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, 2018, 51-52.

CONCLUSIONES

- Ventajas y desventajas de las TIC's:

Las TIC's han supuesto un gran avance y tienen influencia en todos los ámbitos de la vida de las personas, para su desarrollo personal, familiar, laboral, social, de ocio. El mundo tal como lo conocemos hoy día no puede ser concebido sin la utilización de las TIC's, pues son utilizadas en todas las actividades que diariamente realizamos los ciudadanos. Han supuesto un increíble número de ventajas, pero traen consigo unas desventajas reseñables, como la facilidad en cuanto a la comisión de delitos, bien los tradicionales que se abren a nuevas formas comisivas, bien la aparición de nuevas figuras delictivas que tienen como objeto material a los propios sistemas informáticos.

- La persona del hacker:

La primera palabra que se viene a la cabeza en cuanto se menciona la palabra ciberdelito o ciberdelincuencia es hacker. Por mucho que la sociedad se haya esforzado en demonizarlo, un hacker no es un ciberdelincuente. A pesar de que a todas aquellas personas que cometen delitos a través de Internet se les haya denominado como tal. Puede haber muchos perfiles de ciberdelincuentes, no siendo necesario que lleven todos colocada la etiqueta de hacker.

- Es un delito nuevo:

El delito de intrusismo informático es relativamente nuevo, no ha sido hasta 2010 con la reforma de la LO 5/2010 que se introduce por primera vez en el CP. Han sido los organismos internacionales los que han impulsado esta reforma, principalmente desde el Consejo de Europa y la UE ante la necesidad de castigar dicha conducta. La normativa internacional ha de ser el referente a tomar en cuenta para la interpretación del delito de intrusismo informático, pues es la forma de lograr también cierta armonización legislativa entre los distintos países, factor decisivo para la lucha conjunta frente a la ciberdelincuencia.

- Las características del sujeto activo:

Es un acierto que el legislador haya optado por la técnica del delito común en la tipificación de este delito, pues, contra lo que pueda parecer en una primera impresión, para la comisión de este delito de intrusismo informático no es necesario que el sujeto tenga conocimientos especiales. Ha de tenerse en cuenta, además, que cualquier persona puede acceder a

programas o aplicaciones que pueden ser utilizadas para la comisión de un hecho delictivo de estas características.

- Las posibilidades del bien jurídico protegido:

A pesar de la ubicación sistemática, en realidad el delito de intrusismo informático no protege, al menos no de manera inmediata y directa, la intimidad. Esto se confirma si se toma en consideración el objeto material del delito, referido simplemente al acceso al sistema informático, sin necesidad de que el sujeto acceda a datos o informaciones que afecten a la intimidad de su titular. Desde esta perspectiva, por tanto, ha de optarse por la tesis doctrinal que considera que estamos ante un nuevo bien jurídico, de manera inmediata se puede configurar como la confidencialidad de datos y sistemas informáticos, de manera mediata o indirecta forma parte de un bien jurídico supraindividual o colectivo denominado seguridad de los sistemas informáticos.

- Las conductas típicas:

El delito de intrusismo está formado por tres conductas descritas de manera alternativa, el acceso, que puede ser tanto a través de medios tecnológicos o remotos como de manera directa o física, el facilitar a un tercero el acceso, cuya tipificación expresa no era necesaria si ese tercero que accede es una persona no autorizada, pues quien facilita el acceso se castigaría en todo caso como partícipe en el delito, y el mantenimiento en el sistema en contra de la voluntad del titular. Es un acierto que se introduzcan elementos adicionales para restringir el ámbito típico de este delito, como es que el sujeto ha de vulnerar las medidas de seguridad; solo así se está realmente ante una conducta que atenta contra el bien jurídico antes descrito, la confidencialidad como forma de protección última de la seguridad informática.

- La actualización del objeto material:

En la actualidad el delito de intrusismo informático va referido al acceso, facilitar el acceso o mantenerse en el sistema de información, no es necesario que se produzca el acceso a datos o programas contenidos en ese sistema. De esta manera la regulación actual se ajusta de manera más correcta a los textos normativos de los que trae causa, el Convenio de Budapest y la normativa de la UE. Como contrapartida, esto supone un adelantamiento de las barreras de protección del bien jurídico.

- El tipo agravado:

Es un acierto la previsión de la modalidad agravada del delito de intrusismo informático cometido en el seno de una organización o grupo criminal, pues esto obedece a la mayor capacidad delictiva de la organización dedicada a este tipo de actividades. Además de que existe un mayor desvalor de la acción debido a la facilidad que supone realizar estas conductas a través de una organización o grupo criminal.

- La responsabilidad penal de las personas jurídicas:

Una vez que el legislador ha optado por la previsión de la responsabilidad penal de las personas jurídicas, porque las implicaciones económicas de este delito resultan también evidentes, sí es acertada la inclusión del delito de intrusismo informático en el catálogo de delitos que dan lugar a la responsabilidad penal de la empresa. Para que tal responsabilidad surja se han de cumplir alguno de los criterios de atribución de responsabilidad mencionados en el art. 31 CP y que no concurran causas de justificación, en especial, que se haya puesto en marcha el modelo de organización con medidas de vigilancia y control para prevenir delitos.

- La responsabilidad penal del funcionario público:

Se ha previsto un tipo cualificado, lo que no es más que una concreción de la agravante genérica del prevalimiento de la condición de autoridad que tiene el sujeto. Su previsión se considera acertada si se tiene en cuenta el fundamento de esta agravación, la mayor facilidad para cometer el delito y la vulneración de su deber de corrección en el cumplimiento de su cargo, es decir, pues el funcionario ha de aprovecharse de la función que realiza para cometer la conducta delictiva.

- Las dificultades en cuanto a la perseguibilidad del delito:

Los avances legislativos para hacer frente al anonimato que facilitan las TIC’s son más que evidentes, pero siempre ha de hacerse respetando los derechos fundamentales. Por otro lado, la perseguibilidad del ciberdelito se garantiza optando por el principio de ubicuidad.

BIBLIOGRAFÍA

ALMENAR PINEDA, Francisco: *El delito de hacking*, Universitat de Valencia, Valencia, 2017.

- *El delito de hacking*, Aranzadi Thomson Reuters, Cizur Menor (Navarra), 2018.

ALONSO GARCÍA, Javier: *Derecho penal y redes sociales*, Aranzadi Thomson Reuters, Cizur Menor (Navarra), 2015.

ASENCIO GALLEGO, José María: *Los delitos informáticos y las medidas de investigación y obtención de pruebas en el Convenio de Budapest sobre la ciberdelincuencia*, en: ASENCIO MELLADO (dir.)/FERNÁNDEZ LÓPEZ (coord.), *Justicia penal y nuevas formas de delincuencia*, Tirant lo Blanch, Valencia, 2017, 43-67.

BACIGALUPO SAGGESE, Silvina, *Los criterios de imputación de la responsabilidad penal de los entes colectivos y de sus órganos de gobierno (arts. 31 bis y 129 CP)* en: LL 7541 (2011) (se ha utilizado la revista en su formato online).

BARRIO ANDRÉS, Moisés: *La ciberdelincuencia en el derecho español* en: RCG 83 (2011), 273-305.

- *El régimen jurídico de los delitos cometidos en Internet en el derecho español tras la reforma penal de 2010*, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, Aranzadi, Cizur Menor (Navarra), 2012, 31-56.

- *Ciberdelitos: amenazas criminales del ciberespacio*, Reus, Madrid, 2017.

- *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, Wolters Kluwer, Madrid, 2018.

BOLEA BARDON, Carolina: *Del descubrimiento y revelación de secretos*, en: CORCOY BIDASOLO/MIR PUIG (dirs.), *Comentarios al Código Penal. Reforma LO 5/2010*, Tirant lo Blanch, Valencia, 2011, 463-472.

BUJOSA VADELL, Lorenzo M.: *Principios generales del proceso penal ante la persecución de los ciberdelitos: perspectiva española*, en: NAVA GARCÉS (coord.), *Ciberdelitos*, Tirant lo Blanch, Ciudad de México, 2019, 65-81.

CARRASCO ANDRINO, María del Mar: *El delito de acceso ilícito a los sistemas informáticos (art. 197 y 201)*, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, Tirant lo Blanch, Valencia, 2010, 249-256.

CASTELLÓ NICÁS, Nuria: *Delitos contra la intimidad, el derecho a la propia imagen y a la inviolabilidad del domicilio, y delitos contra el honor*, en: MORILLAS CUEVA (dir.), *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, Dykinson, Madrid, 2015, 487-514.

COLÁS TURÉGANO, Asunción: *Nuevas conductas delictivas contra la intimidad (arts. 197, 197 bis, 197 ter)*, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, Tirant lo Blanch, Valencia, 2015, 663-683.

- *El delito de intrusismo informático tras la reforma del CP español de 2015*, en: RBD XXI (2016), 210-229.

DE LA CUESTA ARZAMENDI, José Luis: *Responsabilidad penal de las personas jurídicas en el Derecho español*, en: RPM 5 (2013), 9-33.

DE LA CUESTA ARZAMENDI, José Luis/PÉREZ MACHÍO, Ana Isabel: *Ciberdelincuentes y Cibervíctimas*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 99-120.

DE LA CUESTA ARZAMENDI, José Luis/PÉREZ MACHÍO, Ana Isabel/SAN JUAN GUILLÉN, César: *Aproximaciones criminológicas a la realidad de los ciberdelitos*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 79-97.

DE LA MATA BARRANCO, Norberto J.: *Ilícitos vinculados al ámbito informático: La respuesta penal*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 15-30.

DE LA MATA BARRANCO, Norberto J./HERNÁNDEZ DÍAZ, Leyre: *Los delitos vinculados a la informática en el derecho penal español*, en: DE LA CUESTA

ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 159-200.

DÍEZ GÓMEZ, Andrés: *El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest*, en: REDUR 8 (2010), 169-202.

DOPICO GÓMEZ-ALLER, Jacobo: *Responsabilidad de personas jurídicas*, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, Francis Lefebvre, Madrid, 2010, 11-38.

FERNÁNDEZ BERMEJO, Daniel/MARTÍNEZ ATIENZA, Gorgonio: *Ciberseguridad, ciberespacio y ciberdelincuencia*, Aranzadi Thomson Reuters, Cizur Menor (Navarra), 2018.

FERNÁNDEZ HERNÁNDEZ, Antonio: *Organizaciones y grupos criminales (arts. 570 bis, 570 ter, 572 y 574)*, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, Tirant lo Blanch, Valencia, 2015, 1345-1354.

FERNÁNDEZ TERUELO, Javier Gustavo: *Cibercrimen. Los delitos cometidos a través de Internet. -estafas, distribución de pornografía infantil, atentados contra la propiedad intelectual, daños informáticos, delitos contra la intimidad y otros delitos en la Red-*, Constitutio Criminalis Carolina, Oviedo, 2007.

- *Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*, Lex Nova, Valladolid, 2011.

GARCÍA RIVAS, Nicolás/LAMARCA PÉREZ, Carmen: *Organizaciones y grupos criminales (arts. 570 bis, 570 ter y 570 quáter)*, en: ÁLVAREZ GARCÍA/GONZÁLEZ CUSSAC (dirs.), *Comentarios a la Reforma Penal de 2010*, Tirant lo Blanch, Valencia, 2010, 503-520.

GIMÉNEZ SOLANO, Vicente Miguel: *Hacking y ciberdelito*, Universitat Politècnica de Valencia, Valencia, 2011.

GONZÁLEZ COLLANTES, Tàlia: *Los delitos contra la intimidad tras la reforma de 2015: Luces y Sombras*, en: RDPC 13 (2015), 51-84.

GONZÁLEZ CUSSAC, José Luis: *Responsabilidad penal de las personas jurídicas (arts. 31 bis, ter, quáter, quinquies)*, en: GONZÁLEZ CUSSAC (dir.)/GÓRRIZ ROYO/MATALLÍN EVANGELIO (coords.), *Comentarios de la Reforma del Código Penal de 2015*, 2ª, Tirant lo Blanch, Valencia, 2015, 151-210.

HERNÁNDEZ DÍAZ, Leyre: *Aproximación a un concepto de derecho penal informático*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 31-54.

- *Los accesos ilícitos a sistemas informáticos. Normativa internacional y regulación en el ordenamiento penal español*, Aranzadi, Cizur Menor (Navarra), 2019.

LUZÓN PEÑA, Diego-Manuel: *Lecciones de Derecho Penal. Parte general*, 3ª, Tirant lo Blanch, Valencia, 2016.

MATELLANES RODRÍGUEZ, Nuria: *Algunas razones para la represión penal autónoma del intrusismo informático*, en RICPC XXVI (2005), 131-136.

MIRÓ LLINARES, Fernando: *Delitos informáticos. Hacking. Daños*, en: ORTIZ DE URBINA GIMENO (coord.), *Memento Experto. Reforma penal 2010. Ley Orgánica 5/2010*, Francis Lefebvre, Madrid, 2010, 141-167.

- *El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid, 2012.

- *Cibercrimen y vida diaria 2.0*, en: MIRÓ LLINARES/AGUSTINA SANLLEHÍ/MEDINA SARMIENTO/SUMMERS (eds.), *Crimen, oportunidad y vida diaria. Libro homenaje al Profesor Dr. Marcus Felson*, Dykinson, Madrid, 2015, 415-455.

MORALES GARCÍA, Oscar: *Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248)*, en: QUINTERO OLIVARES (dir.), *La Reforma Penal de 2010: Análisis y Comentarios*, Aranzadi, Cizur Menor (Navarra), 2010, 181-193.

- *Comentarios a los delitos informáticos de los arts. 197, 248 y 264 CP*, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, Aranzadi, Cizur Menor (Navarra), 2012, 151-165.

MORALES PRATS, Fermín: *La tutela penal de la intimidad: privacy e informática*, Destino, Barcelona, 1984.

MORILLAS CUEVA, Lorenzo: *La cuestión de la responsabilidad penal de las personas jurídicas*, en: Anales de Derecho 29 (2011), 1-33.

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

PALAZZI, Pablo A.: *El delito de acceso ilegítimo a un sistema informático*, en: DUPUY (dir.)/ KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, BdeF, Buenos Aires, 2018, 37-56.

PÉREZ ESTRADA, Miren Josune: *La investigación del delito a través de las nuevas tecnologías. Nuevos medios de investigación en el proceso penal*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 305-319.

PÉREZ MACHÍO, Ana Isabel: *Dos problemas particulares de cara a la persecución de los delitos informáticos*, en: DE LA CUESTA ARZAMENDI (dir.)/DE LA MATA BARRANCO (coord.), *Derecho penal informático*, Aranzadi, Cizur Menor (Navarra), 2010, 247-278.

PORRES ORTIZ DE URBINA, Eduardo: *Responsabilidad penal de las personas jurídicas*, en https://elderecho.com/responsabilidad-penal-de-las-personas-juridicas-tribuna (consultado en fecha 17 de octubre de 2020).

RAYÓN BALLESTEROS, María Concepción/GÓMEZ HERNÁNDEZ, José Antonio: *Cibercrimen: particularidades en su investigación y enjuiciamiento*, en: AJEE 47 (2014), 209-234.

RODRÍGUEZ GARCÍA, Nicolas: *Análisis de la regulación legal de la responsabilidad penal de las personas jurídicas*, en: *Los Retos del Poder Judicial ante la sociedad*

globalizada: Actas del IV Congreso Gallego de Derecho Procesal (I Internacional), 2012, 197-232.

RUEDA MARTÍN, Mª Ángeles: *Protección penal de la intimidad personal e informática (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código Penal)*, Atelier, Barcelona, 2004.

- *Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales*, en: ROMEO CASABONA/GUANARTEME SÁNCHEZ LÁZARO (eds.)/ARMAZA ARMAZA (coord.), *La adaptación del derecho penal al desarrollo social y tecnológico*, Comares, Granada, 2010, 347-379.

- *La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la intimidad y la propia imagen*, en: Indret 4 (2013), 1-40.

SIERRA LÓPEZ, Mª del Valle: *Los delitos de descubrimiento y revelación de secretos en el Código Penal de 2015: artículos 197, 197 bis, 197 ter, 197 quáter, 197 quinquies y 198*, en: DEL CARPIO DELGADO (coord.), *Algunas cuestiones de parte especial tras la reforma de 2015 del Código Penal*, Tirant lo Blanch, Valencia, 2018, 133-186.

SUÁREZ-MIRA RODRÍGUEZ, Carlos/JUDEL PRIETO, Ángel/PIÑOL RODRÍGUEZ, José Ramón: *Descubrimiento y revelación de secretos*, en: AAVV, *Delincuencia informática. Tiempos de cautela y amparo*, Aranzadi, Cizur Menor (Navarra), 2012, 167-175.

TEMPERINI, Marcelo: *Delitos informáticos y cibercrimen: técnicas y tendencias de investigación penal y su afectación a los derechos constitucionales*, en: DUPUY (dir.)/KIEFER (coord.), *Cibercrimen II. Nuevas conductas penales y contravencionales. Inteligencia artificial aplicada al Derecho penal y procesal penal. Novedosos medios probatorios para recolectar evidencia digital. Cooperación internacional y victimología*, BdeF, Buenos Aires, 2018, 219-254.

TEVENET GUTIÉRREZ, Manuel Ángel: *Art. 197 bis y recomendaciones para la prevención de los ciberdelitos contra la intimidad*, Universitat Oberta de Catalunya, Barcelona, 2019.

TOMÁS-VALIENTE LANUZA, Carmen: *Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente)*, en: IDP 27 (2018), 30-41.

VELASCO NÚÑEZ, Eloy/SANCHIS CRESPO, Carolina: *Delincuencia informática. Tipos delictivos e investigación. Con jurisprudencia tras la reforma procesal y penal de 2015*, Tirant lo Blanch, Valencia, 2019.

VIDAURRI ARÉCHIGA, Manuel: *Delitos informáticos. Los retos del derecho penal*, en: NAVA GARCÉS (coord.), *Ciberdelitos*, Tirant lo Blanch, Ciudad de México, 2019, 197-220.