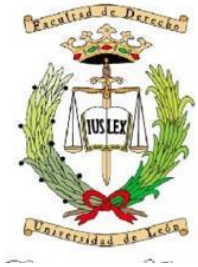
universidad de león



FACULTAD DE DERECHO
UNIVERSIDAD DE LEÓN
CURSO 2018/2019

CIBERDELITOS. EL DELITO DE INTRUSISMO INFORMÁTICO EN EL ORDENAMIENTO JURÍDICO ESPAÑOL.

CYBERCRIMES. THE CRIME OF HACKING IN THE SPANISH LEGAL ORDER.

GRADO EN DERECHO

AUTOR: ÓLIVER DE LA FUENTE FERRERAS

TUTORA: ISABEL DURÁN SECO

ÍNDICE

ABREVIATURAS

Art/s	Artículo/s
Coord/s	Coordinador/es
BOE	Boletín Oficial del Estado
CE	Constitución Española
CP	Código Penal
Dir/s	Director/es
DM	Decisión Marco
Ed	Edición
FD	Fundamento de Derecho
INCIBE	Instituto Nacional de Ciberseguridad
IP	Internet Protocol
LO	Ley Orgánica
LOPJ	Ley Orgánica del Poder Judicial.
Núm.	Número
OEDI	Observatorio Español de Delitos Informáticos
ONU	Organización de las Naciones Unidas
OSCE	Organización para la Seguridad y la Cooperación en Europa
PC	Personal Computer
SAP	Sentencia de la Audiencia Provincial
STS	Sentencia del Tribunal Supremo
TIC/s	Tecnología/s de la Información y Comunicación
TUE	Tratado de la Unión Europea
TFUE	Tratado de Funcionamiento de la Unión Europea
VPNs	Virtual Private Network
UE	Unión Europea

RESUMEN/ABSTRACT

El desarrollo que ha experimentado Internet y las nuevas tecnologías en el siglo XXI ha supuesto nuevos retos para el Derecho. Las TICs se encuentran en pleno auge, por lo que cada día surgen nuevas técnicas que permiten acceder a la información de manera más sofisticada, teniendo en cuenta que, progresivamente, las personas físicas y jurídicas archivan en la red datos pertenecientes a la esfera pública y privada; esto conlleva el nacimiento de nuevas modalidades delictivas vinculadas a dicha innovación tecnológica; como consecuencia, aumentan los riesgos para las posibles víctimas, que carecen de un perfil concreto. Por otra parte, la figura del *hacker* tradicional ha evolucionado hasta el punto de poder establecer una clasificación por grupos en función de su actividad. Por todo ello, el presente trabajo versa sobre las principales características de los ciberdelitos y su incidencia en nuestro ordenamiento jurídico. Del mismo modo, nos centraremos en las reformas con mayor trascendencia del CP español, efectuadas en 2010 y 2015 respectivamente, así como las consecuencias derivadas de los mismos. Concretamente, hice hincapié en el análisis del intrusismo informático que, por sus particularidades, es el delito informático más común y, además, supone el instrumento para cometer otras conductas delictivas.

Palabras clave: Ciberdelincuencia, hacker, intrusismo informático, delitos informáticos.

The development that the Internet and new technologies have experienced in the 21st century has presented new challenges for the Law. TICs is in full swing, so that new techniques are emerging every day that allow access to information in a more sophisticated way, taking into account that, progressively, natural and legal people file data belonging to the public sphere on the network private; this entails new criminal modalities' birth linked to this technological innovation; as a consequence, risks increase for potential victims, who lack a specific profile. On the other hand, the traditional hacker's figure has evolved to the point of being able to establish a classification by groups according to their activity. For these reasons, this paper deals with the main characteristics of cybercrime and its impact on our legal system. In the same way, we will focus on the reforms with greater importance of the Spanish Criminal Code, carried out in 2010 and 2015 respectively, as well as consequences derived from them. Specifically, I focused on the analysis of hacking, which, due to its peculiarities, is the most common computer crime and, in addition, it is the instrument to commit other criminal behaviors.

Keywords: Cybercrime, hacker, hacking, computer crimes.

OBJETO DEL TRABAJO

Actualmente, nos hallamos inmersos en una realidad que ha experimentado una revolución tecnológica sin precedentes en los últimos años. La irrupción vertiginosa de las TICs en todos los aspectos y ramas del conocimiento ha traído aparejada la superación de algunas barreras técnicas que en el siglo pasado parecían insuperables. Ahora bien, es verdad que cualquier innovación conlleva una multitud de utilidades potenciales, susceptibles de ayudar y solventar muchos problemas de la sociedad; o, por el contrario, puede servir de instrumento para cometer acciones punitivas que causen daños o perjuicios a terceros. Llegados a este punto, no está de más recordar que los objetos o instrumentos no son ni buenos ni malos en sí mismos, sino que depende del uso que la persona haga de ellos de acuerdo con su intencionalidad. Hoy en día, cualquier sujeto puede ser portador de un *Smartphone, tablet* o cualquier otro dispositivo que nos permite enviar y recibir información en tiempo real; sin embargo, existen demasiadas evidencias a favor de poder afirmar que una gran parte de la sociedad no está lo suficientemente sensibilizada con los peligros potenciales que se derivan de su mal uso. Sin ir más lejos, las compras online o las redes sociales nos posibilitan adquirir productos o entablar conversaciones con otras personas de forma casi instantánea, en nuestra zona de confort, o sea, nuestro propio hogar, sin necesidad de desplazamientos o pérdidas de tiempo. Pero, a su vez, estamos compartiendo aspectos de nuestra intimidad o datos de carácter económico que antes de la aparición de dichas herramientas resultaban casi imposibles de conseguir para los delincuentes.

El nacimiento de la cibercriminalidad ha establecido una nueva serie de retos para el Derecho penal material, completamente novedosos en cuanto que se ha superado la barrera del espacio físico y nos movemos en un espacio estrictamente virtual, concepto inimaginable hace solo algunas décadas. En conclusión, retos completamente distintos a los que se afrontaban con los delitos tradicionales. Las estadísticas del OEDI nos muestran una tendencia al alza desde 2014 hasta el momento presente de la comisión de ciberdelitos (ver Anexo 1), por lo que urge cada vez con mayor premura la adopción de una serie de medidas y actuaciones necesarias que sean capaces de frenar este avance. Dentro de estos nuevos tipos penales, se valora como el de mayor relevancia al referido como intrusismo informático o *hacking*, el cual, además de considerarse el delito más

común en sí mismo, presenta la característica de ser el vehículo para la comisión de otras conductas ilícitas vinculadas a los sistemas de información. Se puede concretar la importancia de este delito aludiendo al ejemplo del ransomware[1] WannaCry, sucedido el 12 de mayo de 2017. Se trató de uno de los peores ataques *hacker* de la historia, que tuvo como consecuencia la paralización de miles de empresas en todo el mundo y puso de manifiesto la fragilidad del sistema ante determinados ataques, llegando a afectar a más de 170 países[2].

Una vez que hemos llegado a este punto, puedo afirmar que el objetivo general del presente trabajo consiste en dar respuesta a la siguiente pregunta: ¿Cómo puede afrontar el Derecho penal los riesgos derivados del avance de las nuevas tecnologías que ha experimentado la sociedad actual?

Lógicamente, se trata de una pregunta que tiene una enorme trascendencia para los actuales miembros de la sociedad, caracterizada entre otras cosas, por ser global y cambiante a un ritmo vertiginoso. Para ir aproximándonos a la obtención de una respuesta, será necesario proceder a la resolución de una serie de cuestiones con carácter previo, que pueden concretarse en la formulación de los siguientes objetivos:

- Analizar la evolución de las TICs desde su origen hasta la actualidad.
- Delimitar y caracterizar la ciberdelincuencia, ciberdelitos o delitos informáticos.
- Conocer el tratamiento de los ciberdelitos en el ámbito internacional con el Convenio Europeo sobre ciberdelincuencia y, especialmente, en el ámbito de la Unión Europea con la DM 2005/222/JAI y la Directiva 2013/40/UE.
- Estudiar la trayectoria de los ciberdelitos en nuestro ordenamiento jurídico, con las reformas operadas en el CP a través de la LO 5/2010 y la LO 1/2015, que introducen la regulación principal sobre esta materia para dar respuesta a la normativa internacional y de la UE, expuesta en el párrafo anterior.

[1]*Tipo de software mal intencionado (malware) que básicamente "secuestra" (encripta) toda la información que hay en un ordenador, como archivos, documentos, etc., y después pide una remuneración económica para su "rescate" (descifrar)*. Definición extraída de RAMOS MOROCHO, Raúl Armando/ GALLEGOS MOSQUERA, Enrique: *3c Tecnología: glosas de innovación aplicadas a la pyme*, 2016, 68.
[2]AVAST. Extraído de https://www.avast.com/es-es/c-wannacry. Visto el 20 de junio de 2019.

- Analizar la evolución del delito de *hacking* o intrusismo informático, introducido por primera vez en nuestro ordenamiento jurídico en 2010, así como la forma en que ha variado su tratamiento en las sucesivas reformas.
- Señalar las principales posturas doctrinales en relación a las insuficiencias que presenta nuestro ordenamiento jurídico con respecto a la regulación de este tipo de delincuencia, en general; y del intrusismo informático o *hacking* (197 *bis* 1), en particular.

METODOLOGÍA

El filósofo Emilio Bunge fue capaz de condensar en una sola frase la relación existente entre la ciencia y el método científico, al expresar de forma contundente: "Donde no hay método científico no hay ciencia" (Bunge, 1976).

De esta afirmación se puede deducir y definir, a la vez, el concepto de investigación científica como la acción de aplicar el método científico.

Puesto que existen varias ramas del saber que confluyen en determinadas disciplinas o ciencias, el método científico se adecua a las peculiaridades de cada una de ellas, pero sin perder la esencia de su verdadera razón de ser, que no es otra que la de llegar al conocimiento objetivo.

Dado que nuestro objeto de estudio se halla dentro del marco jurídico, obviamente será la investigación jurídica la empleada en la resolución de conflictos derivados del mero hecho de pertenecer a una realidad social que va más allá de la suma de los individuos que la forman, para adentrarse, concretamente, en el tipo de relaciones que mantienen entre ellos.

Centrándome ya en el presente trabajo, voy a proceder a realizar un recorrido por todas las fases del proceso que han dado lugar a la elaboración del mismo.

1. Selección del tutor, tema y puntos clave a tratar

Una vez elegida la profesora que ejercería como tutora del presente trabajo, le comuniqué mi deseo de abordar las cuestiones relacionadas con la ciberdelincuencia. Seguidamente, asistí a unas reuniones en las que se nos proporcionaron las pautas a seguir para efectuar correctamente los aspectos de índole formal, tales como citas a pie de página y referencias a los distintos tipos de obras y materiales utilizados para llevar a

cabo la actividad en cuestión. Posteriormente, elaboré una propuesta de trabajo que envié para que fuera supervisada y corregida. Fue en ese punto concreto cuando la tutora me sugirió que me centrara en el delito de *hacking* para profundizar en él de forma particular. En relación a este delito, he tratado cuestiones que tienen difícil solución como la referida al bien jurídico protegido y que ha dado lugar al surgimiento de posturas enfrentadas o corrientes distintas entre los expertos en la materia.

2. Fuentes de información y documentación

Tras las pertinentes correcciones y sugerencias, la tutora me indicó la bibliografía que me podía servir como fuente para la elaboración del documento final. Procedí, pues, a la lectura de los libros recomendados y de toda la normativa legal que, directa o indirectamente, versaba sobre el tema. Además, consulté diversas páginas web relacionadas con la cuestión y analicé los datos estadísticos proporcionados por el OEDI.

3. Redacción del texto

Una vez concluida la fase anterior, realicé una reflexión sobre los aspectos estudiados y procedí, posteriormente, a redactar con la mayor coherencia posible el presente documento, tomando como hilo conductor la reciente aparición del delito de intrusismo informático y su posterior evolución dentro del ámbito más generalizado de la ciberdelincuencia. Concretamente, se introduce a través de la LO 5/2010 y se reforma mediante la LO 1/2015.

Además, incluí en el mismo una revisión de la reducida jurisprudencia existente en relación al delito de *hacking*, que consiguió despejar ciertas dudas sobre cuestiones controvertidas para la propia doctrina.

Finalmente, envié el documento a la tutora por epígrafes y, una vez corregidos, mantuvimos varias reuniones en las que me expuso los fallos encontrados y me orientó acerca de cómo subsanarlos. Después de tener en cuenta todas las apreciaciones realizadas, le remití el texto completo, que fue objeto de una última revisión y corrección final. Tras tomar en consideración las últimas instrucciones dadas, procedí a trasladar de nuevo el trabajo íntegro a la profesora, quien, por fin, emitió el visto bueno. Como paso previo a la exposición y defensa del mismo, llevé a cabo su depósito.

PARTE CENTRAL DEL TRABAJO

1. Introducción

Hoy en día todos somos conscientes de la trascendencia que tiene Internet en nuestras vidas; no solo referida a la incidencia directa en el área personal y profesional de cada individuo y que, por extrapolación, se extiende a todos los ámbitos de la sociedad, sino también al enorme peso que ejerce sobre el desarrollo de la economía global y que vuelve a repercutir de nuevo, aunque sea de forma indirecta, sobre las personas que integran los grupos sociales[3]. Este instrumento nos ha permitido acceder a la información casi en tiempo real; es decir, los acontecimientos se producen y se divulgan al mismo tiempo. Dicha información es, además de accesible, susceptible de ser modificada, copiada y distribuida a un número infinito de potenciales emisores; hecho que supone un avance técnico sin precedentes en la historia de la humanidad. Sin pretender menoscabar su impacto en nuestro tiempo, la era tecnológica ha ido mostrando paulatinamente sus puntos negativos, la contrapartida de las ventajas que nos ha proporcionado. Definitivamente, el hombre ha tomado conciencia del inmenso poder que supone el uso y manejo de información; se ha convertido en el arma más eficaz, tanto a nivel defensivo como ofensivo[4].

Día tras día, seguimos experimentando una revolución tecnológica acelerada, especialmente en el ámbito de las TICs que, en un corto espacio de tiempo, se convierten en obsoletas porque otras nuevas ocupan su lugar y cumplen funciones más avanzadas que las anteriores. Esto se ha traducido en que tengamos una gran dependencia de ellas en todos los ámbitos de nuestras vidas, puesto que sentimos que, de alguna manera, nos la facilitan, contrarrestan nuestras frustraciones diarias y nos permiten vivir en un continuo "estar conectado al mundo", que nos da la sensación de sentirnos más seguros[5].

Como se acaba de apuntar, a pesar de todas las bondades que ha traído este desarrollo tecnológico, viene acompañado, como contrapartida, de una serie de riesgos[6] que, dado el carácter trasnacional y universal de los medios de comunicación, facilitan la comisión de conductas ilícitas a través de los mismos. Es por ello que, en el ámbito penal, la

[3]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 212.
[4]BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 17-19.
[5]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 18-20.
[6]MAYER LUX, Laura: *Ius et Praxis*, 2018, 161.

evolución de la política criminal plantea una renovación legislativa con carácter necesario y urgente a raíz de la ineficacia de los mecanismos de tutela actuales para dar respuesta a las necesidades derivadas de tales conductas[7].

Sin embargo, y a pesar de todo lo expuesto con anterioridad, no podemos olvidar el principio de intervención mínima y de *última ratio* que operan dentro del Derecho penal[8]. Expresado de otro modo, la sola existencia de una conducta de riesgo en relación con las tecnologías y sistemas de información, no implica necesariamente la utilización de un instrumento punitivo. Es por ello que las acciones que deben ser competencia de esta disciplina son las que vulneran los intereses de la forma más grave y no cualquier acción o conducta de riesgo[9].

En relación con todo lo anterior, dentro de nuestro ordenamiento jurídico, el tratamiento de la ciberdelincuencia no puede entenderse sin dos reformas esenciales que ha sufrido nuestro CP de 1995, en 2010[10]y en 2015[11]. Estas reformas buscan acomodar la normativa de la UE en el ámbito de los ciberdelitos y, a su vez, la política llevada a cabo para dar respuesta a los mismos[12]. Si observamos las estadísticas que maneja el OEDI en relación con la comisión de este tipo de delitos, solo desde el año 2016 al 2017, han pasado de contabilizarse 66.586 a 81.307; tendencia que, presumiblemente, continúe aumentando en los próximos años, dada su trayectoria ascendente[13]. Por ende y a tenor de la amplia casuística que representan este tipo de conductas ilícitas, el objeto del presente trabajo se centra especialmente en el intrusismo informático o *hacking*, puesto que se trata del delito más frecuente y se configura como el principal medio para llevar a cabo la comisión de otros ilícitos penales[14].

---

[7]Véase entre otros: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 27-30; ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 20-21.

[8]ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 254.

[9] COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 212.

[10]Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Publicado en el BOE núm. 152, de 23 de junio de 2010.

[11]Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Publicado en el BOE núm. 77, de 31 de marzo de 2015.

[12]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 213.

[13]Datos disponibles en http://oedi.es/estadisticas/, consultado el 11 de mayo de 2019.

[14]Al respecto: COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 212-214; ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 21-23.

2. Antecedentes

Antes de adentrarnos en el concepto de delito informático, considero que es relevante mencionar con carácter previo, el germen de esta revolución tecnológica.

A pesar de que las TICs están omnipresentes en nuestra vida y continúa creciendo su poder en todos los aspectos, el surgimiento de las mismas y, en especial, el de Internet, tienen su origen en el siglo pasado. Concretamente en 1958, el Departamento de Defensa de los Estados Unidos creó la Agencia de Proyectos de Información Avanzada para superar tecnológicamente a la antigua Unión Soviética, en el contexto histórico conocido como " Guerra Fría". Su finalidad era captar recursos del ámbito universitario para aplicarlos al mundo militar. Sin embargo, no será hasta 1972 cuando empiecen a surgir los primeros resultados relevantes con la materialización de ARPANET (del inglés *ARPA*: *Advanced Research Projects Agency, y NET: hace referencia a la red*), primer programa de conmutación de paquetes creado en 1969[15]. Precisamente, es en 1972 cuando este programa se hace público y se introduce su primera aplicación: el correo electrónico. A partir de aquí, ARPANET continúa su evolución hacia la conexión con otros ordenadores, hecho que da lugar a la aparición de Internet. En la actualidad, la red se nos presenta como una integración descentralizada[16].

La expansión del uso de Internet se generaliza a partir de los años 90, momento que supone la llegada a la población con carácter general[17]. Ello permitió el acceso e intercambio de una gran cantidad de información proveniente de cualquier parte del mundo. Lo que parecía un beneficio para la sociedad sin precedente, se vio enturbiado con la transmisión de información prohibida entre países a una velocidad nunca antes alcanzada. Por otra parte, el acceso a la pornografía infantil, a la apología del racismo o a la xenofobia, constituían potencialmente uno de los peligros asociados a la nueva ciberdelincuencia. Hay que hacer una mención especial al término *hacking* o intrusismo informático, el cual sigue aumentando de manera exponencial actualmente. A esto hay que añadir el desarrollo de nuevas modalidades delictivas como el envío masivo de

[15]ALONSO, Enrique: *Factótum: Revista de Filosofía*, 2017, 86.
[16]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 27-28.
[17]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 45.

correos electrónicos no solicitados a particulares, empresas o instituciones, con finalidades e intereses diversos[18].

La llegada de Internet supuso la elevación de los delitos informáticos, ya existentes previamente, desde el ámbito local o regional hasta un nuevo ámbito global, dado que no solo se incrementan las formas tradicionales de delincuencia, sino que se perfeccionan las nuevas formas de ciberdelincuencia, esto nos deja entrever que la misma ha pasado a ser uno de los principales problemas para los países, organizaciones y ciudadanos, los cuales se encuentran en una situación en la cual el ordenamiento jurídico no protege adecuadamente los intereses públicos y privados. Ello y, especialmente por el incremento de los ciberataques y el desarrollo frenético de las tecnologías, unido al carácter internacional, ha llevado a los Estados a cooperar entre sí en materia de ciberdelincuencia[19].

Hasta ahora, hemos hablado del origen de Internet y del desarrollo, en general, de los medios de comunicación. Sin embargo, no es posible entender el devenir de los acontecimientos hasta el día de hoy sin definir la figura del *hacker*, puesto que el origen de los delincuentes cibernéticos lo podemos encontrar en estos sujetos. Los *hackers* se atribuían el deber ético de compartir la información y facilitar su acceso siempre que fuera posible[20]. Sus actuaciones se movían por un afán de conocimiento y estrictamente dentro de los límites de la legalidad. Hoy en día, los intereses de todo tipo han tergiversado a esta figura; no obstante, hay que distinguir a los *white hat* (sombreros blancos), que representan al perfil tradicional del mismo, de los *black hat* (sombreros negros) y *grey hat hackers* (sombreros grises), los cuales se han puesto al servicio del crimen organizado. Los sombreros negros son aquellos *hackers* que acceden a los sistemas informáticos ajenos, beneficiándose de sus vulnerabilidades. En contraposición a la figura anterior, tenemos a los sombreros blancos[21], los cuales llevan a cabo actividades para detectar los fallos de los sistemas informáticos e informar a sus distribuidores con el objetivo de subsanar las posibles deficiencias[22]. Por último, los sombreros grises son aquellos que se encuentran entre las dos figuras anteriores, detectan por un lado las vulnerabilidades de los sistemas informáticos y avisan a la

[18]Al respecto: ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 60; también en: El delito de hacking, 2018, 40-41.
[19]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 61-62.
[20]MAYER LUX, Laura: *Ius et Praxis*, 2018, 182.
[21]Desde la reforma del CP de 2010, el hacking blanco es una conducta punible
[22]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 214.

comunidad *hacker* y a los distribuidores de esos productos, a la vez que observan las consecuencias. Por tanto, desaparece el perfil de delincuente para dar lugar a un elenco de perfiles que van a tener como denominador común el uso de las TIC con acceso a Internet[23].

3. La ciberdelincuencia. Clasificación de los ciberdelitos y principales características

El concepto de ciberdelincuencia es bastante reciente en relación al surgimiento de Internet. Desde que se produce la revolución de los medios de comunicación, las personas más versadas en el tema han discutido sobre cuál es el término que mejor se adapta a esta nueva forma de delincuencia y qué rasgos característicos la definen[24].

Los primeros trabajos doctrinales que abordan estas cuestiones surgen a partir de la década de los 70 del siglo pasado, momento en el que se intenta dar respuesta a un conjunto de fenómenos que tienen como denominador común la utilización de sistemas informáticos, ya sea utilizándolos como medios para cometer delitos o como fines en sí mismos; es decir, siendo los objetivos a los que se dirige la transgresión. En este punto hay que resaltar que en España, dicho fenómeno ocurrió una década después que en los países más avanzados en nuevas tecnologías[25]. El objetivo en este momento era poner sobre el mapa la irrupción de un nuevo modelo de criminalidad ligada a la utilización de redes telemáticas, bien sea contra los propios sistemas, contra los datos informáticos o contra los programas que, en algunos casos, suponían nuevos tipos de conductas antijurídicas ya conocidas, y que en otros supuestos fue necesario ampliar dicha tipología para abarcar esos comportamientos aún no contemplados. Sin embargo, para la mayoría de los expertos en este tema, no existe una clase autónoma que englobe el delito informático; puesto que, más que definir un espacio jurídico común a todos ellos, se centra en un ámbito de riesgo[26].

Esta falta de acuerdo para delimitar el concepto de ciberdelincuencia queda claramente reflejada en el seno de la UE y, más concretamente, en la Comunicación de la Comisión

[23]Sobre ello: BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 33-36; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 41-42; ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 59.
[24]Véase entre otros: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 33-35; ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 28-29.
[25]Al respecto: BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 24-31; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 33-35.
[26]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 212-213.

al Parlamento Europeo, al Consejo y al Comité de las Regiones (COM (2007) 267 final) de 22 de mayo. En ella, se refleja la importancia que supone la lucha contra la ciberdelincuencia, entendiéndola como un elemento básico cuya presencia es innegable en nuestras sociedades. También deja entrever la falta de entendimiento entre los juristas en relación a qué concepto se ajusta mejor a este nuevo tipo de delincuencia. A falta de una definición comúnmente aceptada de ciberdelincuencia, los términos ciberdelincuencia, delincuencia informática, delincuencia relacionada con los ordenadores o delincuencia de alta tecnología se utilizan a menudo indistintamente. Una vez expresados los sinónimos que engloba el vocablo de ciberdelincuencia, nos aporta una definición de la misma la aludida Comunicación de la Comisión en su epígrafe 1.1: así, "*por ciberdelincuencia se entienden las actividades delictivas realizadas con ayuda de redes de comunicaciones y sistemas de información electrónicos o contra tales redes y sistemas"*[27].

De dicha definición podemos extraer que este concepto comprende tres tipos de modalidades delictivas: en primer lugar, las formas tradicionales de delincuencia, como el fraude o la falsificación; aunque específicamente alude a delitos cometidos a través de redes electrónicas. En segundo lugar, alude a la publicación de contenidos ilegales (material que incite al terrorismo, xenofobia, racismo o pornografía infantil, entre otros). Por último, el tercer tipo engloba delitos específicos de las redes electrónicas, íntimamente relacionados con las nuevas tipologías delictivas, sobre los cuales verse el presente trabajo. Esta última modalidad comprende conductas como ataques contra sistemas informáticos, denegación de servicios y la piratería[28]. La nota común y de mayor relevancia de estos tres tipos de delitos es que pueden cometerse a gran escala y es posible una gran distancia geográfica entre el hecho delictivo y los efectos producidos[29].

Por todo lo expuesto con anterioridad, esta clasificación hace hincapié en la distinción entre las conductas delictivas cometidas a través de la informática y los delitos en los que la informática, en sí misma, es el objeto del delito. La doctrina, a raíz de las peculiares características de los ciberdelitos (fácil comisión, escasos recursos y fácil

[27]Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM (2007) 267 final de 22 de mayo de 2007).
[28]Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité de las Regiones: Hacia una política general de lucha contra la ciberdelincuencia (COM (2007) 267 final de 22 de mayo de 2007).
[29]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 28.

accesibilidad a los mismos en relación con los perjuicios causados; posibilidad de cometerlos en otra jurisdicción sin estar presente físicamente y aprovechamiento de las lagunas normativas de algunos Estados en este tema, que pueden denominarse paraísos cibernéticos), es partidaria y defiende cada vez con mayores argumentos la definición de ciberdelincuencia dentro de la legislación penal de unos bienes jurídicos distintos vinculados a la informática[30].

No obstante, para los principales autores no existe una clasificación unitaria de los ciberdelitos, por lo que solo aludiré a aquellas más relevantes. Así pues, el primer criterio clasificador es el que diferencia si el sistema informático es un instrumento o medio para cometer otros delitos; o bien, es el propio objetivo del delito. Esta distinción ha sido objeto de cierta controversia, en cuanto que se discute si una conducta típica consistente en la utilización de un ordenador para cometer otro tipo delictivo es o no delito informático. La segunda clasificación que tiene trascendencia para el presente trabajo es la que distingue entre los delitos que se desarrollan en Internet y los delitos efectuados sobre instrumentos tecnológicos como ordenadores. Aquí, por la propia orientación de este trabajo, haré especial hincapié en los delitos cometidos a través de los medios tecnológicos[31].

La heterogeneidad que caracteriza estas conductas delictivas, su naturaleza especial y la dificultad para llevar a cabo su persecución han obligado a los Estados a armonizar el Derecho penal material entre sí[32].

4. Obstáculos que dificultan la persecución de la ciberdelincuencia

En consecuencia y a tenor de las razones y características expuestas previamente, los ciberdelitos se presentan como un fenómeno en el que no existe un bien jurídico común afectado, sino que en realidad podemos referirnos a una zona de riesgo, como consecuencia de la generalización de las nuevas tecnologías y que es común a numerosos bienes jurídicos protegidos. Por ende, la primera característica definitoria radica en el peligro para los bienes jurídicos más relevantes, como pueden ser la libertad sexual, la intimidad o el patrimonio[33]. Además de los bienes jurídicos tradicionales,

[30]BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 24-31.
[31]DÍAZ GÓMEZ, Andrés: *REDUR*, 2010, 181-182.
[32]Al respecto: ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 28; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 33-35.
[33]En este sentido: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 37; MAYER LUX, Laura: *Ius et Praxis*, 2018, 194.

surgen otros nuevos susceptibles de daños potenciales, como puede ser la seguridad de los propios sistemas informáticos[34].

El segundo rasgo característico es la enorme facilidad[35] para llevar a cabo este tipo de comportamientos, donde las conductas emitidas de forma remotas apenes pueden dejar rastros del ataque, con las consecuentes dificultades para su persecución y posterior castigo. Uno de los principales dilemas a los que se enfrenta la ciberseguridad es la detección y persecución de los delitos por las propias características del espacio virtual que constituye Internet. El primer obstáculo a sortear en este terreno es la determinación de la autoría de los ciberdelitos que, en principio, no sería muy difícil identificar cualquier dispositivo conectado a Internet a través de su dirección IP. Sin embargo, aunque se trate de un dato público y de carácter personal, existen medios que permiten dificultar su identificación, tales como la conexión a través de redes *wi-fi* abiertas o la utilización de la red *Tor* (The Onion Router), entre otros[36].

En tercer lugar, conviene reseñar que las conductas pueden llevarse a cabo sin límites fronterizos, hecho que facilita su impunidad. Otro de los grandes problemas referentes a la persecución de estos delitos reside en aquellos cometidos en otros países y en la competencia territorial para reconocerlos como tales[37]. No se puede obviar que el desarrollo de Internet guarda una estrecha relación con la globalización, razón por la cual va a suponer un problema ubicar la comisión de un delito, ya que puede originarse en uno o varios países y, a su vez, el daño puede materializarse en otro u otros. Trasladando todo lo anterior a efectos jurídicos, el mayor problema reside en poder determinar la competencia jurisdiccional, a tenor del artículo 23.1 de la LOPJ[38], que establece el principio de territorialidad como regla general[39]. A todo ello, hay que añadir factores tales como la ausencia de inmediación entre el autor y la víctima, además de la despersonalización o la inexistencia de un ordenamiento supranacional.

---

[34]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 35.
[35]DÍAZ GÓMEZ, Andrés: *REDUR*, 2010, 174-176.
[36]Sobre ello: ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 36; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 37-43.
[37]MAYER LUX, Laura: *Ius et Praxis*, 2018, 165.
[38]**Artículo 23.**
1. *En el orden penal corresponderá a la jurisdicción española el conocimiento de las causas por delitos y faltas cometidos en territorio español o cometidos a bordo de buques o aeronaves españoles, sin perjuicio de lo previsto en los tratados internacionales en los que España sea parte*.
[39]Véase entre otros: ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 36; BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 43-48; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 51-52.

Por último y como nota aclaratoria, es necesario afirmar que en la modalidad de acceso ilícito, existe cierta vulnerabilidad de los equipos y sistemas informáticos que los convierte en potencialmente accesibles y, por otro lado, los sujetos que cometen tales actos manifiestan poseer un alto grado de especialización en el tema[40].

5. Regulación a nivel supranacional de los ciberdelitos contra la intimidad

Dentro del ámbito trasnacional, las circunstancias cada vez más apremiantes han obligado a los distintos países a adoptar soluciones de carácter internacional. Actualmente, existe una tendencia colaboradora para tratar la ciberseguridad de una forma conjunta; aunque esto no es óbice para que los territorios mantengan un interés especial por contar con herramientas propias que les permitan y, a su vez, les garanticen mantener su independencia y seguridad[41]. Antes de adentrarme en el fondo del asunto de este apartado, resulta prioritario que aporte una breve definición del concepto que entraña el vocablo de ciberseguridad. Podemos entender dicha palabra como "*la protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, se almacena o transporta mediante los sistemas de información interconectados*". La acepción de ciberseguridad comprende aquellas actuaciones que tienen como objetivo reforzar la seguridad de las redes, sistemas de información y de comunicación que componen el ciberespacio; a la vez que detectan y combaten por los medios pertinentes las intrusiones e incidentes acaecidos en dicho espacio virtual; todo ello con la finalidad de preservar la confidencialidad, disponibilidad e integridad de la información[42].

Así pues, no es de extrañar que los Estados comenzaran a ser conscientes del peligro potencial que entrañaban las redes y sistemas de comunicación e información desde el siglo pasado. Es en ese momento cuando la carencia de una normativa internacional y la falta de adaptación de las legislaciones nacionales al carácter transnacional de la ciberdelincuencia, obligó a la toma de conciencia de la gravedad del problema[43]. Un primer atisbo de respuesta lo encontramos dentro de la esfera de la ONU, institución que publicó en 1977 el Manual de las Naciones Unidas para la Prevención y Control de Delitos informáticos, más conocido como *Manual Tallin*; además de otra serie de

[40]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 35.
[41]FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: Ciberseguridad, ciberespacio y ciberdelincuencia, 2018, 88.
[42]FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: Ciberseguridad, ciberespacio y ciberdelincuencia, 2018, 88.
[43]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018. 62.

medidas para el mismo fin. Por otra parte, en el seno de la Organización para la Seguridad y la Cooperación en Europa (OSCE) han sido aprobadas una serie de normas encaminadas a reducir los riesgos de posibles conflictos que pueden surgir con la utilización de las TICs; así como facilitar e impulsar la comunicación de los Estados que forman parte de dicho organismo y mejorar la protección de las infraestructuras[44].

Conviene recordar en este punto que la capacidad de la UE para poder legislar dentro del ámbito del Derecho penal es limitada[45]. Sin embargo, aunque sus competencias están orientadas prioritariamente a la organización comercial, la delincuencia puede suponer un obstáculo a las actividades comerciales entre los distintos Estados miembros, hecho que le ha permitido disponer de una competencia parcial para la regulación del Derecho penal. Algunos de los cambios más importantes introducidos se refieren tanto al Tratado de Maastricht (1993) como al de Ámsterdam (1997), que afectaron al ámbito de la justicia y de los asuntos de interior (JAI)[46].

Por lo que respecta al artículo 83.1[47]del TFUE permite a la UE adoptar medidas directivas cuyo contenido sean normas mínimas que definan las infracciones penales y las sanciones, siempre que se trate de delitos especialmente graves y que tengan una dimensión transfronteriza. Además, el Consejo podrá decidir que se añadan más delitos a la lista. Dentro del apartado 2º del citado artículo[48], se contempla la posibilidad de adoptar directivas como en el apartado 1, pero referidas a delitos menos graves. A todo

[44]Véase entre otros: ASENCIO MELLADO, José Mª (dir.) / FERNÁNDEZ LÓPEZ, Mercedes (coord.): Justicia penal y las nuevas formas de delincuencia, 2017, 46; BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 52-54; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 59.

[45]BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 62.

[46]Véase entre otros: ASENCIO MELLADO, José Mª (dir.) / FERNÁNDEZ LÓPEZ, Mercedes (coord.): Justicia penal y las nuevas formas de delincuencia, 2017, 46; BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 52-54; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 59.

[47]*El Parlamento Europeo y el Consejo podrán establecer, mediante directivas adoptadas con arreglo al procedimiento legislativo ordinario, normas mínimas relativas a la definición de las infracciones penales y de las sanciones en ámbitos delictivos que sean de especial gravedad y tengan una dimensión transfronteriza derivada del carácter o de las repercusiones de dichas infracciones o de una necesidad particular de combatirlas según criterios comunes*.

[48]*Cuando la aproximación de las disposiciones legales y reglamentarias de los Estados miembros en materia penal resulte imprescindible para garantizar la ejecución eficaz de una política de la Unión en un ámbito que haya sido objeto de medidas de armonización, se podrá establecer mediante directivas normas mínimas relativas a la definición de las infracciones penales y de las sanciones en el ámbito de que se trate. Dichas directivas se adoptarán con arreglo a un procedimiento legislativo ordinario o especial idéntico al empleado para la adopción de las medidas de armonización en cuestión, sin perjuicio del artículo 76*.

ello, hay que añadir que el artículo 84 del TFUE[49] permite la promoción y el apoyo de acciones en los Estados miembros, quedando excluidas las medidas de armonización[50].

I. Convenio Europeo sobre cibercriminalidad

Son numerosas las medidas llevadas a cabo en este ámbito, aunque me centraré especialmente en aquellas que han tenido mayor trascendencia dentro de nuestro ordenamiento jurídico. En lo que respecta al espacio europeo, la norma de mayor relevancia y la primera que ofrece una respuesta a los ataques criminales contra los sistemas informáticos es el Convenio Europeo sobre cibercriminalidad[51]. Dicho Convenio, aprobado en Budapest el 23 de noviembre de 2001 y vigente desde julio de 2004, se gesta en el marco del Consejo de Europa. A pesar de que entre los países firmantes se encontraba España, aquí no fue ratificado hasta tiempo después, concretamente mediante su publicación en el BOE de 17 de septiembre de 2010, entrando en vigor el 1 de octubre de ese mismo año[52].

Tiene el reconocimiento de ser el primer tratado internacional que hace frente a los delitos informáticos mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y un aumento de la cooperación entre las distintas naciones. Su finalidad es la armonización del Derecho penal material, implantación de medidas procesales o cautelares que estén adaptadas al medio digital y establecimiento de un régimen rápido y eficaz de cooperación internacional[53]. Su creación es la consecuencia del creciente aumento del uso y desarrollo de las TICs, y del elenco de posibilidades que ofrecen estos medios para la comisión de nuevos delitos[54].

Centrándonos en su contenido, ya el preámbulo deja entrever que su finalidad es la de dar respuesta a la creciente necesidad de llevar a cabo una política penal común dirigida

[49]*El Parlamento Europeo y el Consejo podrán establecer, con arreglo al procedimiento legislativo ordinario, medidas que impulsen y apoyen la actuación de los Estados miembros en el ámbito de la prevención de la delincuencia, con exclusión de toda armonización de las disposiciones legales y reglamentarias de los Estados miembros*.

[50]BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 62-63.

[51]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 80.

[52]FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: Ciberseguridad, ciberespacio y ciberdelincuencia, 2018, 167.

[53]En este sentido: FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: Ciberseguridad, ciberespacio y ciberdelincuencia, 2018, 167-168; GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 60-61; MAYER LUX, Laura: *Ius et Praxis*, 2018, 166.

[54]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 80-82; BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 52; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 58-59.

a la prevención de actuaciones efectuadas contra la confidencialidad, la integridad y la disponibilidad de los sistemas de información, redes y datos informáticos y el abuso de los mismos[55]. Para ello, los Estados firmantes se comprometen a introducir en sus respectivas legislaciones las disposiciones contenidas en el capítulo II del Convenio y a manifestar una actitud cooperativa en relación a aquellos asuntos que entren dentro de su ámbito de aplicación[56].

Como ya adelanté en los párrafos anteriores, el Convenio busca crear una base común de delitos con el fin de armonizar el Derecho penal material y, para ello, nos proporciona una definición del mismo (capítulo II, sección 1ª), que comprende *los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*[57]. Otro propósito que merece ser destacado es el de establecer medidas procesales dirigidas a la investigación y obtención de pruebas (capítulo II, sección 2ª); tampoco podemos obviar la necesidad de crear mecanismos que promuevan y faciliten la cooperación internacional (capítulo III). Para finalizar, hay que mencionar el Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos[58].

En definitiva, el Convenio de Budapest de 23 de noviembre de 2001 persigue tres objetivos primordiales en torno a los cuales se estructura: armonizar el Derecho penal material, implantar medidas cautelares o procesales que se adapten al entorno digital y establecer un régimen ágil y eficaz de cooperación internacional[59].

A pesar de todas las bondades que introduce el Convenio Europeo sobre Ciberdelincuencia, también adolece de una serie de fallos, tales como el referido a la redacción de sus preceptos, ya que otorgan un amplio margen de libertad a los ordenamientos internos, dificultando, así, la armonización del Derecho penal material[60].

---

[55]GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 60.
[56]Al respecto: ASENCIO MELLADO, José Mª (dir.) / FERNÁNDEZ LÓPEZ, Mercedes (coord.): Justicia penal y las nuevas formas de delincuencia, 2017, 46; BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 53-54; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 60.
[57]Convenio Europeo sobre ciberdelincuencia.
[58]Al respecto: ARGENTI FERNÁNDEZ, Thais/ PELETEIRO SUÁREZ, Almudena: *Actualidad jurídica Uría Menéndez*, 2011, 40; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 60-61; GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 66-67.
[59]ASENCIO MELLADO, José Mª (dir.) / FERNÁNDEZ LÓPEZ, Mercedes (coord.): Justicia penal y las nuevas formas de delincuencia, 2017, 47.
[60]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 82;

II. DM 2005/222 de 24 de febrero de 2005

La idea de armonización del Derecho penal material que pretendía el Convenio Europeo sobre Ciberdelincuencia, fue concretada en la Decisión marco 2005/222/JAI del Consejo, de 24 de febrero de 2005, relativa a los ataques contra los sistemas de información. En cumplimiento de la misma, se implanta en nuestro CP la reforma introducida por la LO 5/2010, de 22 de junio, referente a una modalidad delictiva por la que se castigan las conductas de acceso y mantenimiento a los datos y programas alojados en un sistema informático (art. 197.3 CP)[61].

Según se expone en su considerando primero, el fin de esta norma consiste en *reforzar la cooperación entre las autoridades judiciales y otras autoridades competentes, incluida la policía y los demás servicios represivos especializados de los Estados miembros, mediante la aproximación de su legislación penal en materia de ataques contra los sistemas de información*[62]. Para lograrlo, se establece la necesidad de legislar los delitos de acceso ilegal a sistemas de información (artículo 2) y delitos de intromisión ilegal en el sistema (artículo 3) o en los datos (artículo 4). Con ello, se pretende evitar una tipificación excesiva de delitos, resaltando la idea de que los objetivos de la DM pueden alcanzarse de manera más satisfactoria dentro del ámbito de la UE, que si se llevaran a cabo medidas legislativas de carácter individual por parte de los Estados miembros.

En la DM surge de nuevo el mismo problema que ya presentaba el Convenio Europeo sobre cibercriminalidad, puesto que las directrices marcadas adolecen nuevamente de ser muy laxas y permisivas en relación con las conductas potencialmente lesivas como el *hacking*. Los Estados, una vez cumplidos los mínimos exigidos por la misma, han podido decidir los elementos del tipo delictivo, alejándose aún más del objetivo de armonización y coordinación en esta materia[63].

III. Directiva 2013/40/UE

La Decisión marco 2005/222/JAI fue sustituida en 2013 por la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. Esta nueva directiva incorpora otras exigencias en

[61]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 214.
[62]La Decisión marco 2005/222/JAI del Consejo de 24 de febrero de 2005 relativa a los ataques contra los sistemas de información.
[63]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 84.

materia de protección de los sistemas de información, así como diferentes estrategias para la coordinación de las autoridades competentes[64].

El objetivo de la directiva se encuentra en los considerandos y en el artículo 1, el cual dispone: *La presente Directiva establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información*[65]. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades competentes. Su redacción deja entrever la importancia de los sistemas de información dentro de la UE para el normal desarrollo de las interacciones sociales, políticas y económicas[66].

La Directiva va a imponer a los Estados miembros la obligación de adoptar medidas necesarias y urgentes en relación a las conductas ilícitas contenidas en sus artículos 3 (Acceso ilegal a los sistemas de información), 4 (Interferencia ilegal en los sistemas de información), 5 (Interferencia ilegal en los datos) y 6 (Interceptación ilegal). Por tanto, se vuelve a incluir el acceso ilícito y se incorpora la interceptación ilegal, ampliando las conductas previstas con carácter previo en la DM 2005/222[67].

6. Tratamiento de la ciberdelincuencia en el Derecho penal español

Es necesario exponer, en primer lugar, que para la regulación sustantiva de los ciberdelitos operan dos técnicas normativas que presentan la característica de ser opcionales: por un lado, el recurso a leyes penales especiales y, por otro, la tipificación de nuevas figuras delictivas en el Código Penal. Por la primera, han optado países como Francia, Gran Bretaña, Chile o Venezuela; mientras que se han decantado por la segunda técnica países como Alemania, Austria, Italia, Portugal y España. Por otra parte, dentro del ámbito procesal, los estados más avanzados han empezado a acomodar

[64]Al respecto: COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 214; CONCEPCIÓN OBISPO, Triana: *Revista Aranzadi Doctrinal*, 2017, 183; GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 60-61.
[65]Directiva 2013/40/ UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.
[66]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 85-87.
[67]Directiva 2013/40/ UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información.

aquellas medidas de investigación contenidas en las leyes procesales penales referidas a la utilización de las TICs con una finalidad delictiva[68].

España ha sido uno de los países que ha optado por la regulación de la ciberdelincuencia en el propio CP. Sin embargo, ni el CP de 1973, ni el actual de 1995, incluidas sus sucesivas reformas, han dedicado un Título o rúbrica específica para los delitos informáticos. A todo ello, hay que mencionar la técnica de formulación normativa utilizada, ya que se optó por modificar y extender el ámbito de aplicación de los delitos tradicionales frente a la creación de tipos delictivos autónomos. La extensión de los tipos delictivos clásicos se llevó a cabo a través de dos vías: en primer lugar, dentro de los delitos tradicionales se introdujeron subtipos autónomos con el fin de penar las nuevas modalidades ilícitas. En segundo lugar, se produjo una extensión del ámbito de los objetos materiales de aquellos delitos que guardaban alguna analogía con los nuevos hechos punibles[69].

Hay que destacar la reforma del CP de 2010[70], que en relación a los ciberdelitos se ha limitado a modificar conductas susceptibles de reproche penal y a introducir otras nuevas[71]. Dentro de los principales tipos afectados, hay que hacer hincapié en el *hacking* o intrusión informática (197.3 CP)[72], la estafa informática (248 CP), el *cracking* o daños informáticos (264 CP) y el nuevo delito de embaucamiento a menores o *childgrooming* (183 bis CP)[73]. La justificación de esta reforma se fundamenta en la necesidad de armonizar la legislación interna con la normativa internacional y suplir las carencias de nuestro CP en relación con los delitos informáticos. La reforma del CP de 2010, como se puede desprender de su preámbulo, sirve para cumplir las disposiciones de la DM 2005/222/JAI y agrupa en dos apartados

[68]Sobre ello: BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 51-52; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 57-58.
[69] Véase entre otros: BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 55-57; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 67.
[70]Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[71]Al respecto: ARGENTI FERNÁNDEZ, Thais/ PELETEIRO SUÁREZ, Almudena: *Actualidad jurídica Uría Menéndez*, 2011, 40-41; GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 67-68.
[72]Tras la reforma operada por la LO 5/2010, el artículo 197.3 CP tipifica por primera vez el delito de hacking. Posteriormente, como veremos más adelante se ha vuelto a modificar con la reforma de la LO 1/2015.
[73]BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 68.

las conductas punibles; así, nos permite distinguir los daños informáticos del delito de *hacking*[74].

En 2015 se produce una gran reforma de nuestro CP. Como consecuencia de la misma, se revisa el régimen de penas y su aplicación; se adoptan mejoras técnicas para ofrecer un sistema penal más rápido y coherente; se añaden nuevos tipos de conductas punibles y se reforman los ya existentes; y, por último, desaparecen las conductas tipificadas como faltas. Esta reforma viene motivada por la necesidad de ofrecer una respuesta a la delincuencia informática y se lleva a cabo a través de la trasposición de la Directiva 2013/40/UE, ya mencionada en los párrafos anteriores[75]. En relación con el cibercrimen, la reforma abarca la pornografía infantil y recoge el castigo correspondiente a través de la inclusión de un nuevo apartado, que contiene las sanciones para aquellas personas que accedan a través de TICs a este tipo de pornografía. Por esta misma razón, se faculta de forma expresa a jueces y tribunales para que puedan ordenar la adopción de medidas para el bloqueo o retirada de aquellas páginas web que lo contengan[76].

La reforma del CP de 2015 ha venido a ampliar la regulación establecida por la del 2010, mediante la incorporación de las nuevas exigencias derivadas de la Directiva. Por lo que se refiere a los delitos que vamos a analizar en este trabajo, se ha mantenido la regulación dentro del capítulo dedicado a la tutela de la intimidad y la ha ampliado con la incorporación de nuevas figuras. La reforma del CP introducida por la LO 1/2015 tiene su justificación en cuanto que ofrece una respuesta a la delincuencia informática en el mismo sentido que la normativa europea, mediante la trasposición de la Directiva 2013/40/UE[77].

Así pues, se continúa incluyendo dentro de los delitos contra la intimidad el llamado delito de intrusismo informático, que cambia su ubicación del art. 197.3 CP al art. 197 *bis* 1 y, a su vez, se añaden otros dos nuevos: el delito de interceptación de trasmisiones no públicas de datos informáticos (Art. 197 *bis*. 2), y el que castiga la producción o

[74]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 78-79.
[75]En ese sentido: ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 87; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 663-664; GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 52-53; GIL ANTÓN, Ana María: *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2017, nº 39, 1-2.
[76]Sobre ello: BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, 2017, 57-58; también en: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 68-69.
[77]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 88-89.

facilitación de instrumentos para la realización de los actos delictivos, comprendidos en los artículos 197. 1, 2 y 197 *bis* (Art. 197 *ter*)[78].

En definitiva, podemos decir que las últimas reformas han puesto de manifiesto la ausencia de un criterio sistemático compartido para ubicar este tipo de conductas, tanto por parte del legislador nacional como por el comunitario. Frente al caos que ha producido la creación y sucesión interminable de normas comunitarias que han modificado esta materia de un modo más bien anárquico, una parte de la doctrina considera que deberían haber realizado una única norma comunitaria, capaz de regular las conductas básicas de la delincuencia informática y de aportar claridad, congruencia y orden; y que, posteriormente, se llevase a cabo el desarrollo de aquellas cuestiones accesorias o técnicas que fueran surgiendo a tenor de la rápida transformación de las nuevas tecnologías[79].

7. Ciberdelitos contra la intimidad y derecho a la propia imagen: especial atención al delito de hacking o intrusismo informático

Nuestra Carta Magna reconoce dentro del artículo 18[80]el derecho a la intimidad personal y familiar, el derecho a la inviolabilidad del domicilio, al secreto de las comunicaciones y a la privacidad informática. El derecho a la intimidad comprende estas cuatro vertientes y tiene por finalidad preservar una esfera de la vida de los ciudadanos que guarda conexión con el respeto a su dignidad como persona (10.1[81] CE), ya sea frente a intromisiones de poderes públicos o particulares [82].

Es en este apartado donde está ubicado el delito de *hacking* o intrusismo informático. Los delitos referidos a la intimidad, al derecho a la propia imagen y a la inviolabilidad

[78]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 214.
[79]ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 2018, 90.
[80]**Artículo 18**

1. *Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
2. *El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
3. *Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
4. *La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

[81]**Artículo 10**
La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.
[82]CASTIÑEIRA PALOU, Mª Teresa/ ESTRADA I CUADRAS, Albert, en: SILVA SÁNCHEZ, Jesús-María (dir.)/ RAGUÉS I VALLÈS, Ramón (coord.): *Lecciones de Derecho Penal. Parte Especial*, 2018, 153-154.

del domicilio están recogidos en el Título X de nuestro CP, que se encuentra dividido en dos capítulos: el primero, relativo al "descubrimiento y revelación de secretos" (arts. 197 a 201)[83]; y el segundo, dedicado al "allanamiento de morada, domicilio de las personas jurídicas y establecimientos abiertos al público" (arts. 202 a 204)[84].

Referente a este título, cabe resaltar la reforma penal acaecida en 2015, puesto que conlleva una serie de modificaciones formales en el ámbito de la tutela de la intimidad, que han dado lugar a una restructuración de las diferentes figuras. Sin embargo, la principal novedad consistió en la propuesta de nuevas conductas delictivas contra la intimidad y contra la seguridad de los sistemas informáticos. Merece una mención especial la introducción de figuras novedosas en el ámbito del intrusismo informático, puesto que se incorpora el concepto de la interceptación ilegal de transmisiones no públicas y se añade por otra parte, el castigo específico para aquellos que faciliten instrumentos para la comisión de la conducta anterior[85]. Al tipificarse de forma expresa una serie de comportamientos susceptibles de reproche penal, basados en la obtención de programas y contraseñas para el acceso a los sistemas informáticos, ha dado lugar a un adelantamiento de la barrera de protección del bien jurídico, que en este caso concreto es la seguridad informática[86].

Dentro de los ciberdelitos contra la intimidad, el más relevante es el referido al intrusismo informático o *hacking* (197.*bis* 1 CP), que pasaremos a analizar a continuación.

El citado artículo dispone lo siguiente: El *que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años*[87]. De la lectura del precepto podemos deducir que la conducta típica del *hacker* es la de aquel sujeto que se vale de su experiencia y conocimientos informáticos con el fin

[83]CASTIÑEIRA PALOU, Mª Teresa/ ESTRADA I CUADRAS, Albert, en: SILVA SÁNCHEZ, Jesús-María (dir.)/ RAGUÉS I VALLÈS, Ramón (coord.): *Lecciones de Derecho Penal. Parte Especial*, 2018, 154.
[84]Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[85] GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 52.
[86]COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): Comentarios a la reforma del Código Penal de 2015, 2015, 663-664.
[87]Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

de vulnerar las medidas de seguridad de un sistema de información. Aunque se trata de un delito común que, en principio, desde un punto de vista formal no exige ninguna condición especial, en la práctica sucede otra cosa distinta, ya que la autoría de los mismos va a implicar a aquellos sujetos que tengan una serie de aptitudes y conocimientos informáticos. En este sentido, podemos afirmar que estamos ante una conducta típica realizada por un especialista informático[88].

I. Bien jurídico protegido

Es destacable la importancia que supusieron las reformas del CP, acaecidas en 2010 y 2015, que introducen y reforman respectivamente el delito de intrusismo informático en nuestro ordenamiento jurídico, para dar cumplimiento a los compromisos de carácter internacional adquiridos para llevar a cabo la tutela de la "seguridad informática"[89].

Una de las cuestiones más controvertidas surge en relación al bien jurídico que se pretende tutelar, que puede ser la seguridad de los sistemas de información, o bien, la intimidad en los sistemas informáticos[90]. La introducción del delito de intrusismo informático planteó en la doctrina la duda sobre cuál es el bien jurídico se pretendía proteger con el mismo[91]. La ubicación elegida por el legislador nacional dentro del capítulo dedicado a la custodia de la intimidad supuso que surgieran dos corrientes doctrinales a la hora de analizar el objeto de tutela[92].

Como consecuencia, una parte de la doctrina argumentaba que la introducción de esta conducta típica supondría el adelantamiento en la protección del bien jurídico referido a la intimidad, el cual corría un riesgo potencial de verse afectado por dichas actuaciones[93]. Por ello, se estableció un cierto paralelismo con el concepto de allanamiento de morada, concretamente con las conductas de entrar y mantenerse, lo

[88]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 215.
[89]Al respecto: COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 671; TOMÁS-VALIENTE LANUZA, Mª del Carmen: *Revista de Internet, Derecho y Política*, 2018, nº 27, 38.
[90]ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 255.
[91]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 118-119.
[92]Véase entre otros: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 110-111; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 91; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 215.
[93]ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 255.

cual deja entrever que lo que se tutela es una parcela de privacidad ligada al domicilio informático[94]. Sobre ello, se pronuncia la SAP de Madrid núm. 985/2017 de 27 de noviembre[95].

Sin embargo, para otros autores, lo que se tutela es la seguridad de los sistemas informáticos[96]. En este sentido, de acuerdo con lo dispuesto en la SAP de Vizcaya núm. 90307/2014 de 23 de julio[97], se entiende que la informática tiene un valor trascendental para la sociedad actual, razón por la cual es necesaria la preservación de la seguridad del tráfico jurídico informático, en general, y la protección de la integridad y confidencialidad de los sistemas informáticos, en particular[98].

En líneas generales, podemos afirmar que la mayoría de la doctrina entendió que el legislador introdujo una figura de peligro abstracto para la seguridad de las redes informáticas que, hipotéticamente, podían suponer un peligro para la intimidad[99].

Resulta evidente que, en la actualidad, la generalización del uso de los ordenadores o cualquier otro dispositivo de naturaleza análoga, ha llevado a que dichos instrumentos almacenen buena parte de nuestra vida personal y privada; en definitiva, nuestra intimidad. Sin embargo, esta esfera relativa a la privacidad ya estaba protegida en

[94]Véase entre otros: ARGENTI FERNÁNDEZ, Thais/ PELETEIRO SUÁREZ, Almudena: *Actualidad jurídica Uría Menéndez*, 2011, 42; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 671-672.

[95]Al respecto: SAP de Madrid, núm. 895/2017 de 27 nov. en su FD 2º párrafo 6: *"Frente a la tesis que sostiene que el bien jurídico protegido en este delito es la seguridad de los sistemas de los sistemas informáticos, cabe defender que la incriminación de esta conducta supone un adelantamiento de las barreras de protección de la intimidad que parte de la consideración de que la mera intromisión informática pone en peligro la privacidad del titular del sistema. Esta interpretación además de atender a la ubicación sistemática del precepto y ser respetuosa con el principio de lesividad, viene refrendada por el propio preámbulo de la Ley Orgánica 1/2015 (LA LEY 4993/2015) que distingue entre "datos que afecta tan directamente a la intimidad personal" y "otros datos o informaciones que pueden afectar a la privacidad pero que no están referidos directamente a la intimidad personal".*

[96]GONZÁLEZ HURTADO, Jorge Alexandre: *Revista Penal de México*, 2016, 70-71.

[97]SAP de Vizcaya, Sección 2ª, Sentencia 90307/2014 de 23 julio de 2014, Rec. 143/2014, en su FD 4º párrafo 5:"*... siendo este delito el denominado de intromisión informática en que lo se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privado de dicha persona*".

[98]En este sentido: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 92; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 215.

[99]Al respecto: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 91-92; COLÁS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 673-674; también en: *Revista Bolivariana de derecho*, 2016, 216-218.

nuestro CP por el art. 197.2[100], el cual engloba toda una serie de conductas que van desde el simple acceso al sistema informático, en el que se encuentran alojados tales datos íntimos, hasta su utilización o modificación[101]. Por ello, el intrusismo informático debía implicar algo distinto a lo que ya se había tipificado previamente en nuestro CP[102]. Además, como ya mencioné en este apartado, la nueva redacción establecida por la reforma del CP en 2015, había supuesto un nuevo adelantamiento en la línea de defensa del bien jurídico, al dejar de exigirse el acceso o mantenimiento, ya fuera a los datos o a los programas alojados en el sistema informático, siendo suficiente que el sujeto activo accediera o se mantuviera en un sistema de información, pero sin llegar a alcanzar dichos datos o programas contenidos en el mismo[103]. Por todo ello, el legislador español debería haber ubicado este delito en un Título distinto al de la intimidad; de esta manera, habría evitado las controversias doctrinales surgidas posteriormente sobre el bien jurídico que es objeto de protección a través de la tipificación del intrusismo informático.

II. Conducta típica

Como ya señalé al analizar el bien jurídico protegido, las conductas que castigaba el art. 197.3 del CP antes de la reforma de la LO 1/2015, de 30 de marzo, coincidían con las que se preveían para el delito de allanamiento de morada puesto que implicaban la condena a aquel sujeto que "*por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, accediera sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantuviera dentro del mismo en contra de la voluntad de quien tuviera el legítimo*

[100]**197.2**. *Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero*.

[101]Véase entre otros: COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 217-218; GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 72.

[102]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 118-119

[103]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 218.

derecho a excluirlo…"[104]. Sobre este aspecto se pronuncia la SAP de Alicante núm. 3591/2015[105].

La doctrina había interpretado hasta ese momento que uno de los requisitos para definir el acceso típico era el quebrantamiento de las medidas de seguridad establecidas para impedirlo, por lo que el acceso a sistemas que carecían de protección suponía una atipicidad, así como el acceso autorizado por el titular del sistema[106]. La cuestión más controvertida apareció en relación a si era necesario o no el acceso lícito inicial, respecto a la conducta de mantenimiento en el propio sistema. Para un sector mayoritario de la doctrina, cuando el acceso ha sido lícito, la ilicitud surge desde el momento en que el sujeto que accedió es requerido para abandonar el sistema y se niega[107], contraviniendo así la voluntad del titular[108].

Con la reforma de 2015 se introducen una serie de cambios referidos al delito de intrusismo informático. La nueva redacción de la figura recogida en el actual art. 197.1 *bis*, dispone lo siguiente: "*El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información*

[104]COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 673.

[105]Al respecto: SAP de Alicante núm. 3591/2015 de 16 de septiembre, FD 3º párrafo 6: *En interpretación de la anterior normativa la Circular de la Fiscalía 1/2011 sobre la reforma Código Penal operada por L.O. 5/2010 de 22 de junio consideraba que la novedad introducida en el art. 197.3 del CP se caracterizaba por la criminalización de las conductas del denominado "hacking", que se define, con cierta similitud al allanamiento de morada, como el acceso a datos o programas informáticos con vulneración de las medidas de seguridad establecidas o mantenerse dentro del programa o sistema, contra la voluntad del titular.*

[106]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 182.

[107]Véase entre otros: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 93; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 676-677; GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 74; ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 270-271.

[108]Véase entre otros: BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 93; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 676-677; GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 74; ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 270-271.

o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años"[109].

En primer lugar, en relación a las conductas ya contempladas desde la reforma de 2010, persiste como frontera de la tipicidad el requisito de ausencia de autorización y que las medidas de protección establecidas sean vulneradas[110]. Se recogen las dos conductas ya conocidas: acceso y mantenimiento; pero, como novedad, se introduce la referencia explícita a un supuesto de colaboración, en cuanto que se tipifica la conducta de aquel que facilita a un tercero el acceso a un sistema de información, bien sea al conjunto o a una parte del mismo[111].

Ello ha dado lugar a una ampliación de las conductas punibles, al elevar al grado de autoría aquellas actuaciones que hasta ese momento solo podían ser comprendidas dentro de los actos de participación, hecho que se tradujo en un castigo desproporcionado y, como consecuencia, muy criticado. En cualquier caso, para que se pueda considerar consumada la conducta del facilitador, es requisito esencial que el acceso al sistema de información se produzca. No parece adecuado tipificar como delito la mera facilitación al acceso sin que se lleve a cabo la actuación concreta, ya que supondría una ampliación de las conductas punibles y, a mayores, traería problemas para poder delimitarlas[112] dentro del nuevo art. 197*ter*[113].

Así pues, y para concretar lo expuesto anteriormente, se sanciona el acceso o facilitación del mismo sin autorización, a través de cualquier medio o procedimiento, y siempre que se vulneren las medidas de seguridad operativas para impedirlo; ya sea a

---

[109]Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[110]En ese sentido: SAP de Madrid núm. 16438/2017 de 27 de noviembre, FD 2º, párrafo 9*:(...) Siendo suficiente para colmar las exigencias del tipo el mero acceso al sistema informático que puede ser directo o remoto pero debe haberse realizado vulnerando las medidas de seguridad establecidas para impedirlo.*

[111]Al respecto: COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 219; ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 272; SIERRA LÓPEZ, Mª del Valle, en: DEL CARPIO DELGADO, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, 2018, 174-175.

[112]GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 74

[113]**Artículo 197 ter.**
Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:
a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

datos o programas informáticos contenidos en un sistema de información; o bien mantenerse dentro del mismo en contra de la voluntad del titular. Por tanto, se trata de un tipo mixto alternativo, que integra las conductas de acceso, facilitación o mantenimiento. Se trata, pues, de un tipo delictivo llevado a cabo por instrumentos, medios o procedimientos indeterminados. Su estructura típica se corresponde con la de un delito de peligro abstracto, ya que no requiere que la conducta afecte a la intimidad del titular del sistema, sino que basta que se menoscabe la seguridad del mismo[114].

Por último, conviene destacar que nos encontramos ante un delito doloso; lo que significa que el sujeto que lleve a cabo la conducta punible tiene que manifestar la intención de quebrantar las medidas de protección de los sistemas de información, con la finalidad de vulnerar la seguridad de los mismos. La conducta será atípica si el acceso es el resultado de un descuido o negligencia en la que no hay intencionalidad[115].

III. Objeto material

El objeto material también ha sufrido una serie de modificaciones. En la LO 5/2010 el art.197.3 del CP hacía referencia a que el acceso o el mantenimiento solo se consumaba cuando se proyectaba sobre datos o programas contenidos en un sistema informático o en parte del mismo[116].

Sin embargo, en la reforma establecida por la LO 1/2015, el legislador modificó el objeto material del delito. Así pues, en la nueva redacción que define al precepto, las conductas han de efectuarse sobre el conjunto o una parte de un sistema de información, sin que sea necesario el acceso efectivo a los datos o programas que se contienen en el mismo. Como consecuencia, se produce un adelantamiento en la barrera de protección del bien jurídico, que no es otro que la seguridad en los sistemas de información. En este sentido encontramos jurisprudencia que respalda esta interpretación como la SAP

[114] BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 93.

[115]COLÁS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 678; también en: *Revista Bolivariana de derecho*, 2016, 220.

[116]En este sentido: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 139-140; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 220. También se pronuncia sobre ello la SAP de Madrid núm. 6026/2015 de 27 de abril, en su FD tercero, subapartado B), párrafos 12 y 13: *Este nuevo subtipo, sanciona el acceso inconsentido a informaciones ubicadas en el sistema informático (datos, programas..) o el simple mantenimiento en páginas web ajenas, sin consentimiento del titular, sin necesidad de móvil o acción posterior alguna, y se castiga con pena de hasta dos años. Se castiga, pues, el mero hecho de saltarse las barreras de seguridad informáticas, como un atentado al derecho a la "intimidad informática" pero siempre que exista un acceso a los datos o programas albergados.*

de Salamanca, núm. 37/2018 de 29 junio. Por tanto, la conducta punible es el mero acceso al sistema informático, aún sin acceder a los programas o datos comprendidos dentro de ese sistema[117].

El cuerpo normativo que nos ofrece una respuesta clarificadora de los términos a los que me he referido anteriormente, es la Directiva Europea 2013/40/UE, la cual contiene una definición de sistemas de información y datos informáticos, regulados en su artículo 2, apartados a) y b), respectivamente. En cuanto al primer término, la Directiva lo define como: "*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 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*"[118]. Por lo que respecta a los datos informáticos, los describe 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*"[119]. Por ello, podemos deducir que, desde un punto de vista conceptual, la Directiva distingue entre sistemas de información, refiriéndose en este caso al aparato o conjunto de aparatos que almacenan los programas: y, por otra parte, alude a los datos informáticos, que se procesan a través de los primeros[120].

Las variaciones o modificaciones a las que he aludido anteriormente vienen explicitadas en la exposición de motivos de la ley de 2015 y tienen por finalidad superar las limitaciones de la legislación vigente hasta ese momento, para dar respuesta a la delincuencia informática en el mismo sentido de la normativa europea[121].

---

[117]Al respecto: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 140; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 94; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 220.

[118]Art. **2.A** de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

[119]Art. **2.B** de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo.

[120]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 143-145; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 221.

[121]SIERRA LÓPEZ, Mª del Valle, en: DEL CARPIO DELGADO, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, 2018, 175-176.

IV. Sujetos y pena prevista

Nos encontramos ante un tipo delictivo común que, en principio, puede ser cometido por cualquier persona; si bien es cierto que, por las particularidades del hecho punible, lo más normal es que se lleve a cabo por cualquiera que tenga unos conocimientos especiales en la materia[122]. Por tanto, aunque potencialmente el sujeto activo pueda ser cualquier persona, la conducta concreta, en determinados casos, presenta una cierta complejidad de carácter técnico que implica una mínima cualificación para poder realizarse de forma intencionada[123].

Por otra parte, el sujeto pasivo es el titular de un sistema informático o una parte del mismo, que ha sufrido la conducta punible, ya sea de acceso o mantenimiento. Puede ser tanto una persona física como jurídica, a tenor de lo dispuesto en el art. 200[124]del CP[125].

En cuanto a la pena prevista para este delito, la reforma de 2015 no prevé ningún cambio, por lo que se mantiene la prisión de 6 meses a 2 años[126].

V. Relaciones concursales

El estudio de estas relaciones se llevará a cabo desde la perspectiva de los supuestos que son más habituales, en concurrencia con el delito tratado en el presente trabajo. A raíz de las características que componen el *hacking*, encontramos un amplio elenco de delitos que puede ser precedido por un acceso de carácter ilícito a un sistema informático[127]. A pesar de todo ello, me he centrado en las situaciones concursales más comunes, que son las siguientes.

1. Intrusismo informático y la conducta contenida en el art. 197 *ter* del CP

Es posible plantear el delito de entrada a un sistema de información desde un punto de vista anterior a la propia comisión y, más concretamente, en relación concursal con los actos preparatorios que se tipifican en el art. 197 *ter* del CP. La peculiaridad que reviste

[122]Véase entre otros: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 168-169; BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 92.
[123]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 221-222.
[124]**Artículo 200.**
Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.
[125]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 169-170.
[126]BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, 2018, 95.
[127]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 238.

este último radica en que la acción alude al hecho de proporcionar instrumentos concretos para el acceso, que comprende programas informáticos, contraseñas de ordenador o un código para acceder al mismo. A tenor de la ambigüedad que supone la redacción de este precepto, permite plantear la concurrencia entre los supuestos de facilitar el acceso previsto en el art. 197 *bis* 1 del CP y las conductas típicas que comprende el mismo[128].

En este caso, se produce la confluencia de un concurso de normas que, en principio, se debería resolver en virtud del principio de especialidad, tratado en el art. 8 del CP[129], a favor del art. 197 *ter* del CP[130]. No obstante, en la práctica esta solución es difícil de aplicar, puesto que, según lo dispuesto en el art. 197 *ter* del CP, llevaría en última instancia a resolver el concurso en atención al criterio en que se produzca el acceso de forma efectiva. No obstante, en la mayoría de supuestos surgirá un inadecuado solapamiento de ambos tipos delictivos, que por su difícil delimitación se aplicaría, en cualquier caso, el art. 197 *ter* del CP[131].

Un caso aparte es el referido al supuesto en el que la persona facilita los medios necesarios para la comisión del intrusismo informático y, al mismo tiempo, es el actor del mismo[132]. En dicha situación, parece más correcto considerar la conducta como un delito continuado de acceso ilícito[133].

2. Intrusismo informático (197 *bis* 1 del CP) y el allanamiento de morada de los arts. 202.1 y 203.1 del CP

El delito de *hacking* comprende cualquier conducta que implique un acceso a un sistema de información, ya sea de carácter remoto o físico, que posibilita la existencia de un

[128]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 234-235.
[129]**Artículo 8:** *Los hechos susceptibles de ser calificados con arreglo a dos o más preceptos de este Código, y no comprendidos en los artículos 73 a 77, se castigarán observando las siguientes reglas:*
1. ª El precepto especial se aplicará con preferencia al general.
2. ª El precepto subsidiario se aplicará sólo en defecto del principal, ya se declare expresamente dicha subsidiariedad, ya sea ésta tácitamente deducible.
3. ª El precepto penal más amplio o complejo absorberá a los que castiguen las infracciones consumidas en aquél.
4. ª En defecto de los criterios anteriores, el precepto penal más grave excluirá los que castiguen el hecho con pena menor.
[130]CONCEPCIÓN OBISPO, Triana**:** *Revista Aranzadi Doctrinal*, 2017, 188.
[131]Al respecto: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 234; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 680.
[132]GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 77.
[133]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 235.

concurso entre dos hechos delictivos: el acceso ilícito, tratado en el art. 197 *bis* 1 del CP y el allanamiento de morada, incluido en los arts. 202.1 y 203.1 del CP[134].

En el caso expuesto anteriormente, si partimos de la modalidad medial, se puede deducir que el acceso físico al sistema informático, como infracción más grave, absorbe al allanamiento de morada, siempre que se realice en contra de la voluntad de su titular. La situación cambia para el supuesto en el que el acceso a un sistema de información posibilite el control monitorizado del interior de una vivienda o establecimiento puesto que, en este caso, la concurrencia entre ambos delitos será meramente aparente. Sería distinto si para el acceso a una vivienda se utilizara el delito de intrusismo informático como medio necesario para cometer la acción del allanamiento. En este caso, se produciría un concurso medial[135].

3. El art. 197 *bis* 1 y las conductas del art. 197.2 del CP

Ante esta relación concursal, también es posible que la entrada ilícita a un sistema de información pueda tipificarse como delito, según lo regulado en el art. 197.2 del CP. Este último incorpora elementos subjetivos del injusto, mientras que para el art. 197 *bis* 1 de nuestro CP, no se requiere una intencionalidad específica[136]. En estos casos, en términos generales, se puede apreciar un concurso medial del artículo 77 del CP. No obstante, en el supuesto de que una persona llegase a acceder a un sistema informático apoderándose de datos de carácter reservado o, bien, accediera a ellos sin autorización, se produciría un concurso de normas entre los delitos comprendidos en el art. 197 *bis* 1 y el art. 197.2 del CP, que se resolvería por la vía del art. 8.3 del CP, quedando el primero absorbido por este último[137].

4. Intrusismo informático del art. 197 *bis* 1 y las conductas del art. 264 del CP

[134]**202.1**. *El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años*.
203.1. *Será castigado con las penas de prisión de seis meses a un año y multa de seis a diez meses el que entrare contra la voluntad de su titular en el domicilio de una persona jurídica pública o privada, despacho profesional u oficina, o en establecimiento mercantil o local abierto al público fuera de las horas de apertura*.
En este sentido: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 236.
[135]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 236-237.
[136]Véase entre otras: SAP de Pontevedra núm. 2823/2017 de 12 de diciembre; SAP de Madrid núm. 12606/2018 de 14 de septiembre.
[137]Al respecto: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 237; CONCEPCIÓN OBISPO, Triana**:** *Revista Aranzadi Doctrinal*, 2017, 185.

El acceso abusivo a un sistema de información va a suponer un requisito previo, en términos generales, a la comisión de un delito de daños informáticos[138], según lo dispuesto en el art. 264 del CP[139]. Dicha conducta, tras la reforma del CP de 2010, pasa de constituir una tentativa del delito de daños, cuando éstos no se efectúan por causas ajenas a la voluntad del sujeto activo, a la constitución de un delito consumado de *hacking* o intrusismo informático. No obstante, en el caso de que el daño que se pretende llevar a cabo se ejecute de forma efectiva, es decir, una vez que se ha entrado a la red informática de forma ilícita, dará lugar a un concurso ideal en su versión medial. Esto deja entrever que, una vez causado el daño, se absorbería el delito de *hacking* con las consecuencias dispuestas en el art. 77.3 del CP[140]. Sería diferente para el supuesto en el que una vez que se haya consumado el delito de intrusismo informático, se ocasionaran daños en el sistema con posterioridad o, a la inversa, cuando una vez que se han efectuado los daños informáticos con carácter previo, después se llevara a cabo el acceso ilícito, en cuyo caso daría como resultado un concurso real[141].

VI. Disposiciones comunes

Para concluir el análisis de la configuración del delito de intrusismo informático en nuestro ordenamiento jurídico, es necesario abordar una serie de disposiciones relativas al capítulo de "descubrimiento y revelación de secretos", que agravan o extienden la responsabilidad, a los cuales pertenecen: el agravante por actuar en el seno de una organización o grupo criminal (Art. 197 *quater* del CP), la responsabilidad penal de la

[138]SAP de Lleida núm. 201/2018 de 4 mayo, FD segundo, párrafo 2 :*Ahora bien, el delito de daños informáticos tipificado en el artículo 264.1 del CP , en redacción L.O 5/2010 , vigente en el momento de los hechos, precisaba como también ahora como elemento típico que la conducta y el resultado producido fueran graves. Por tanto, para que los hechos enjuiciados pudieran tener verdadera trascendencia penal no basta con que se hubieran borrado, dañado, deteriorado, alteado o suprimido datos, programas o documentos informáticos sino que también es necesario que se hubiera desplegado una conducta grave y, además, que el resultado producido fuera igualmente grave.*

[139]**Artículo 264.1***: El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años.* Sobre ello: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 237; CONTRERAS SOLER, Beatriz/GARRÓS FONT, Imma: *Revista de derecho y proceso penal*, 2017, 134-136.

[140]**Artículo 77. 3:** *En el segundo, se impondrá una pena superior a la que habría correspondido, en el caso concreto, por la infracción más grave, y que no podrá exceder de la suma de las penas concretas que hubieran sido impuestas separadamente por cada uno de los delitos. Dentro de estos límites, el juez o tribunal individualizará la pena conforme a los criterios expresados en el artículo 66. En todo caso, la pena impuesta no podrá exceder del límite de duración previsto en el artículo anterior.*

[141]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 238.

persona jurídica (art. 197 *quinquies* del CP), la responsabilidad del funcionario público (art. 198 del CP) y el carácter semipúblico de este delito[142].

1. La agravación de la responsabilidad penal por actuar en el seno de una organización o grupo criminal (art. 197 *quater* del CP)

A tenor de las exigencias establecidas en la DM 2005/222/JAI, en 2010 se introdujo en nuestro CP una nueva agravación de la pena para aquellos supuestos en los que los hechos delictivos se llevasen a cabo dentro de una organización o grupo criminal. Con la reforma de 2015, se produce, en primer lugar, un cambio en su ubicación, pasando del artículo 197.8 al 197 *quáter*[143] y, en segundo lugar, se extiende, además, a todas las conductas contenidas en el Capítulo I del Título X[144].

De acuerdo con la redacción del ahora derogado art. 197.8 del CP, la cualificación que implicaba ser miembro de un grupo criminal, se proyectaba exclusivamente sobre los delitos de descubrimiento y revelación de secretos y sobre el intrusismo informático[145]. Actualmente, el nuevo contenido permite aplicarlo también a la figuras de quebranto del secreto laboral o profesional[146], en el caso de que dichas conductas delictivas se lleven a cabo en el ámbito de una organización criminal[147].

En resumen, se prevé la imposición de una pena superior cuando los hechos comprendidos en los diferentes apartados de los artículos 197, 197 *bis*, 197 *ter*, 198, 199

---

[142]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 225.

[143]**Artículo 197 *quater.***
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.

[144]Véase entre otros: ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 274; SIERRA LÓPEZ, Mª del Valle, en: DEL CARPIO DELGADO, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, 2018, 182.

[145]CONCEPCIÓN OBISPO, Triana**:** *Revista Aranzadi Doctrinal*, 2017, 188.

[146]**Artículo 199.**
1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.
2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

[147]Al respecto: COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 681; también en: *Revista Bolivariana de derecho*, 2016, 225.

y 200 de nuestro CP, sean cometidos en el seno de una organización o grupo criminal[148].

2. Responsabilidad penal de la persona jurídica (art. 197 *quinquies* del CP*)*

La responsabilidad penal de las personas jurídicas surge por la necesidad de cumplir las obligaciones que contrajo España sobre la armonización jurídica con respecto a las normas de la UE y, en concreto, a través de la DM 2005/222/JAI. Sin embargo, aunque en la citada DM no se dispone expresamente que la responsabilidad exigida tenga que ser de carácter penal, el legislador español en 2010 decidió introducir una cláusula específica de responsabilidad penal de las personas jurídicas[149]. Con la reforma de 2015, la responsabilidad penal de las personas jurídicas va a estar regulada en el artículo 197 *quinquies* del CP, que reproduce el contenido del párrafo segundo del derogado art. 197.3 del CP, el cual contenía la responsabilidad penal de las personas jurídicas por cualquiera de los delitos comprendidos en el antiguo art. 197 de nuestro CP[150]. La nueva redacción dispone: *"Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33"*[151].

Por ello, con la reforma de 2015 estableció la posibilidad de poder exigir responsabilidad penal a las personas jurídicas[152], en relación a las conductas delictivas contenidas en los artículos 197, 197 *bis* y 197 *ter* del CP[153].

---

[148]GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 78.
[149]GONZÁLEZ COLLANTE, Tália: *Revista de derecho penal y criminología*, 2015, 78.
[150]Al respecto: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 296-297; COLAS TURÉGANO, Asunción, en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, 2015, 681; ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 274.
[151]Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal
[152]CASTIÑEIRA PALOU, Mª Teresa/ ESTRADA I CUADRAS, Albert, en: SILVA SÁNCHEZ, Jesús-María (dir.)/ RAGUÉS I VALLÈS, Ramón (coord.): *Lecciones de Derecho Penal. Parte Especial*, 2018, 169.
[153]SIERRA LÓPEZ, Mª del Valle, en: DEL CARPIO DELGADO, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, 2018, 183.

En definitiva, podemos decir que la reforma de 2015 no supuso ningún cambio respecto a la regulación anterior, más allá de los que se derivan de la introducción de nuevos tipos delictivos en el ámbito de los delitos contra la intimidad y la seguridad de los sistemas informáticos, a los que también les será de aplicación la cláusula de responsabilidad penal de los entes societarios[154].

3. Por el carácter de autoridad o funcionario público del sujeto activo

El ordenamiento jurídico añade un agravamiento al hecho delictivo cuando el sujeto activo presenta la condición de ser autoridad o funcionario público.

Su regulación se encuentra comprendida dentro del artículo 198 del CP, que dispone: *"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"*[155].

Dicho precepto no ha sufrido cambios con la reforma de 2015, y se refiere a las conductas realizadas por autoridades o funcionarios públicos cuando actúen fuera de los casos permitidos por la ley, sin que medie una causa legal para efectuar el delito y valiéndose de su cargo para ello[156]. Para algunos autores, el art.198 del CP contiene un delito especial impropio o una alternativa típica agravada por las características del autor. Por tanto, mientras el delito de *hacking* puede ser efectuado por cualquier persona, la conducta penal contemplada en el precepto del art. 198 del CP español supone una agravación de la misma que solo puede llevarla a cabo una autoridad o funcionario público[157].

Llegados a este punto, es necesario establecer una diferenciación entre el artículo mencionado anteriormente y el artículo 417 del CP[158], ya que este último castiga la

[154]COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 225.
[155] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
[156]Al respecto: ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 276-277; COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 226.
[157]ALMENAR PINEDA, Francisco: El delito de hacking, 2018, 291.
[158]**Artículo 417.**
1. La autoridad o funcionario público que revelare secretos o informaciones de los que tenga conocimiento por razón de su oficio o cargo y que no deban ser divulgados, incurrirá en la pena de multa de doce a dieciocho meses e inhabilitación especial para empleo o cargo público por tiempo de uno a tres años.

revelación de secretos o informaciones que no deban ser divulgadas, junto con aquellas que la autoridad o funcionario público haya conocido por razón de su oficio o cargo[159].

4. Delito semipúblico

Conforme a lo previsto en el art. 201 del CP [160], es necesaria la denuncia previa de la persona afectada o de su representante legal por un delito de intrusismo informático para poder iniciar un proceso penal[161]. En el caso de que la víctima sea menor de edad o esté incapacitada, podrá también denunciar de oficio el Ministerio Fiscal. Este requisito no será necesario para el supuesto en el que los hechos sean cometidos por un funcionario público, según lo dispuesto en el art. 198 del CP, ni tampoco cuando el delito pueda afectar a los intereses generales o a un colectivo de personas[162].

Por todo ello, dado su carácter semipúblico, es posible que el ofendido o su representante legal otorguen el perdón, lo que dará lugar a que se extinga la acción

---

Si de la revelación a que se refiere el párrafo anterior resultara grave daño para la causa pública o para tercero, la pena será de prisión de uno a tres años, e inhabilitación especial para empleo o cargo público por tiempo de tres a cinco años.

2. Si se tratara de secretos de un particular, las penas serán las de prisión de dos a cuatro años, multa de doce a dieciocho meses, y suspensión de empleo o cargo público por tiempo de uno a tres años.

[159]SIERRA LÓPEZ, Mª del Valle, en: DEL CARPIO DELGADO, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, 2018, 183-184. Sobre ello, se pronuncia la STS, Sala de lo Penal, núm.1939/2013 de 3 de mayo, en su FD segundo: *La diferencia esencial entre las conductas contempladas en los artículos 197 y 198 y el 417, cometidas por un funcionario o autoridad, se centra en la legalidad del acceso a la información reservada a la que se refieren dichos preceptos. El artículo 197 parte de la exigencia de que el autor no esté autorizado para el acceso, el apoderamiento, la utilización o la modificación en relación a los datos reservados de carácter personal o familiar, castigándose en el artículo 198 a 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. Mientras que el artículo 417 castiga la revelación de secretos o informaciones que no deban ser divulgados, y de los que la autoridad o funcionario público haya tenido conocimiento por razón de su oficio o cargo.*

[160]**Art. 201**

1. *Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.*

2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5º del apartado 1 del artículo 130.

[161]CASTIÑEIRA PALOU, Mª Teresa/ ESTRADA I CUADRAS, Albert, en: SILVA SÁNCHEZ, Jesús-María (dir.)/ RAGUÉS I VALLÈS, Ramón (coord.): *Lecciones de Derecho Penal. Parte Especial*, 2018, 171-172.

[162]Véase entre otros: COLÁS TURÉGANO, Asunción: *Revista Bolivariana de derecho*, 2016, 226; CONCEPCIÓN OBISPO, Triana**:** *Revista Aranzadi Doctrinal*, 2017, 185; ROMEO CASABONA, Carlos María, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel (coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, 2016, 280-281.

penal. Esto no sucede en el caso de que lo concedan los representantes legales de un menor o discapacitado, ya que el juez tiene la potestad de anular la eficacia del perdón, por lo que el Ministerio Fiscal actuará en defensa de los intereses del menor o discapacitado[163].

CONCLUSIONES

Por lo que hemos visto hasta este momento, resulta difícil ofrecer una respuesta clara y contundente al problema de cómo puede afrontar el Derecho penal los riesgos derivados del avance de las nuevas tecnologías que ha experimentado la sociedad actual. No obstante, el estudio y análisis de los conceptos clave que conforman el presente trabajo me ha permitido llegar a las siguientes conclusiones:

I. Necesidad de establecer bases comunes con el fin de dar respuesta al fenómeno de la ciberdelincuencia que, de momento, son insuficientes. Debido a las características de los ciberdelitos expuestas anteriormente, las diferentes Estados y organizaciones se han visto obligados a llevar a cabo medidas para establecer unas bases comunes con el fin de regular y dar respuesta al fenómeno de la ciberdelincuencia. Asimismo, en el ámbito de la UE se han efectuado hasta el momento importantes avances en esta materia, pero claramente insuficientes, especialmente en el marco de la armonización entre las distintas legislaciones de los Estados miembros.

II. Búsqueda de otras soluciones de carácter jurídico distinto. El legislador español ha ido acomodando en nuestro ordenamiento jurídico la normativa internacional y europea a través de las diversas reformas que ha experimentado nuestro CP. Para materializarlo, ha optado por emplear conceptos de carácter indeterminado, con la finalidad de evitar lagunas de punibilidad que puedan surgir con la aparición de nuevos instrumentos

[163]En este sentido: STS, Sala de lo Penal, Sección 1º, núm. 917/2016 de 2 diciembre, FD segundo, apartado 2, párrafos 2 y 3:
Por lo tanto, estamos ante la imposición de un requisito de procedibilidad o de perseguibilidad que permite calificar a estas infracciones penales como semipúblicas (o cuasipúblicas, como también las denomina la doctrina). No son, pues, en principio, delitos públicos y perseguibles de oficio a no ser que se den las circunstancias especiales referidas en el citado precepto.
El legislador sopesa, pues, los derechos e intereses de la persona ofendida o agraviada por el delito y los fines preventivos de la pena y del derecho penal, y permite que la iniciativa corresponda al individuo ofendido y no al Ministerio Fiscal cuando aquél estime que la tramitación del procedimiento supone un menoscabo de su dignidad personal que incrementa los perjuicios que ya de por sí le ocasionó la acción delictiva. Sin embargo, esa perseguibilidad privada es desplazada a manos de la acusación pública en el caso de que concurra un interés general relevante o cuando al afectar el delito a una pluralidad de sujetos se pondere que el conjunto de los derechos subjetivos afectados adquieren una transcendencia social que debe tutelarse con la intervención del Derecho penal.

técnicos. En este sentido, no podemos olvidar el perfil de última *ratio* o de última frontera que caracteriza al Derecho penal; por lo que habrá que buscar otras soluciones de carácter jurídico distintas que no impliquen la tipificación excesiva de conductas susceptibles de reproche penal.

III. El intrusismo informático es el delito más común. A tenor de toda la información que me ha aportado la bibliografía consultada para la elaboración de este trabajo, el delito por excelencia y más frecuente es el que a tantas veces nos hemos referido y que no es otro que el delito de intrusismo informático o *hacking*. Como ya he expuesto en numerosas ocasiones, esta modalidad delictiva se introduce en nuestro ordenamiento jurídico por primera vez en 2010, y reformado con posterioridad, en 2015.

IV. Se castiga el *hacking* blanco y no debería ser una conducta punible. Entre las principales novedades que introduce la mencionada reforma, merece una especial atención el castigo infligido al *hacking* blanco, cuya acción consiste en el mero acceso a un sistema informático. En este sentido, considero que la condena a estas conductas resulta excesiva en relación al peligro o riesgo que comportan, puesto que para hacer efectiva la sanción se ha tenido que adelantar la barrera de protección del bien jurídico que aún no está claramente determinado por la doctrina.

V. El *hacking* no está ubicado correctamente por lo que se debe reubicar. La ubicación del delito de *hacking* en nuestro CP no parece ser la más acertada. Esta afirmación radica en que se encuentra dentro del Título X, Capítulo I, referido al descubrimiento y revelación de secretos. A través de un criterio sistemático, algunos autores entienden que el bien jurídico protegido es la intimidad informática, como se puede extraer del art. 18.4 de nuestra Constitución. Sin embargo, de la redacción del delito, podemos deducir que el bien jurídico que se intenta proteger es la seguridad de los sistemas de información, puesto que constituyen una pieza clave en el ámbito social y, por ello, resulta indispensable para salvaguardarlos, el adelantamiento de la barrera de protección de otros bienes jurídicos. Por tanto, considero que se debería cambiar su ubicación a otro título distinto, con el fin de solventar la controversia doctrinal sobre cuál es el bien jurídico que se pretende proteger.

VI: Desaparición del perfil de víctima para el delito de intrusismo informático. El sujeto pasivo de esta conducta punible puede ser cualquier persona física o jurídica, de cualquier edad, género o condición social, con independencia de que tengan un carácter

público o privado. A ello hay que añadir que, el constante desarrollo que están experimentando las TICs conlleva al aumento potencial de posible afectados. Con ello no pretendo introducir la utopía de que una posible solución sea el abandono de las nuevas tecnologías, sino que resulta imprescindible que las administraciones públicas pongan en marcha programas y medidas que eduquen a la sociedad para que tome conciencia sobre los riesgos y virtudes que se derivan de estos medios. En la actualidad, instituciones como el INCIBE, llevan a cabo este tipo de actuaciones; aunque insuficientes a todas luces debido a la magnitud del problema.

VII: Ciberdelitos con mayor presencia en nuestro ordenamiento jurídico. Los datos estadísticos extraídos del OEDI nos permiten deducir cuáles son los delitos que más presencia tienen en nuestro ordenamiento jurídico, entre los que destaca especialmente el fraude informático por la gran repercusión económica que supuso, concretamente en 2017, y puede suponer para las empresas en el futuro (Ver Anexo 2). El medio necesario para llevar a cabo el fraude informático no es otro que el intrusismo informático, por lo que esta conducta queda subsumida por la primera al tener un mayor reproche penal. Por ende, se puede reafirmar que el intrusismo informático es el delito más común y el medio para cometer otras conductas delictivas.

VIII. No todas las actividades realizadas por *hackers* deben ser conductas punibles. Conviene destacar las connotaciones negativas que se desprenden del término *hacker*. No voy a entrar de nuevo a definir las distintas clases o perfiles que se derivan del mismo, pero sí es necesario destacar la labor realizada por algunos *hackers,* como la organización denominada *Anonymous,* que lucha por la defensa de la libertad de expresión o la independencia de Internet. Por tanto, no podemos criminalizar a todo este colectivo ni, como ya expuse en los párrafos anteriores, utilizar el Derecho penal para castigar todas las conductas del *hacking*, pues algunas reman a favor de los derechos sociales, aunque sean consideradas ilícitas.

IX. Medidas que deberían efectuarse. Por todo ello, podemos concluir que para poder afrontar con éxito los problemas expuestos en este apartado, sería necesario hacer efectivas las siguientes medidas:

- Adecuación del Derecho penal material a las circunstancias que ha establecido la cibercriminalidad.

- Instauración de medidas cautelares de carácter procesal que permitan una rápida y efectiva respuesta por parte del ordenamiento jurídico.
- Puesta en común de un mayor esfuerzo por parte de todos los países que desemboque en una cooperación eficaz.
- Necesidad de impulsar una armonización de las normas más efectiva para optimizar sus resultados.
- Actuaciones pertinentes destinadas a dotar a la sociedad de una mayor sensibilización, con el fin de que las personas tomen conciencia plena de los peligros que conlleva Internet; y, paralelamente, que puedan conocer y emplear mecanismos orientados a la prevención de los mismos.

BIBLIOGRAFÍA

- ALONSO, Enrique: De cómo la Tecnología se hizo Ley. El Gobierno de la Red como modelo tecnopolítico del futuro cercano. *Factótum: Revista de Filosofía*, 2017, nº 18, 85-91.
- ASENCIO MELLADO, José Mª (dir.)/FERNÁNDEZ LÓPEZ, Mercedes (coord.): Justicia penal y las nuevas formas de delincuencia, Tirant lo Blanch, Valencia, 2017.
- ALMENAR PINEDA, Francisco: Ciberdelincuencia: Teoría y práctica, 1ª ed., Juruá, Porto, 2018.
- ALMENAR PINEDA, Francisco: El delito de hacking, 1ª ed., Aranzadi, Cizur Menor (Navarra), 2018.
- ARGENTI FERNÁNDEZ, Thais/ PELETEIRO SUÁREZ, Almudena: Luces y sombras de dos de los nuevos delitos introducidos con la reforma penal de 2010: el acoso laboral (mobbing) y el intrusismo informático. *Actualidad jurídica Uría Menéndez*, 2011, nº 29, 28-48.
- BARRIO ANDRÉS, Moisés: Ciberdelitos: Amenazas criminales del ciberespacio, Reus, Madrid, 2017.
- BARRIO ANDRÉS, Moisés: Aspectos penales, procesales y de seguridad de los ciberdelitos, Wolters Kluwer, Madrid, 2018.
- CASTIÑEIRA PALOU, Mª Teresa/ ESTRADA I CUADRAS, Albert: Tema 7 Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, en: SILVA SÁNCHEZ, Jesús-María (dir.)/ RAGUÉS I VALLÈS, Ramón (coord.): *Lecciones de Derecho Penal. Parte Especial*, 5ª ed. Atelier, Barcelona, 2018, 153-171.
- COLÁS TURÉGANO, Asunción: El delito de intrusismo informático tras la reforma del CP Español de 2015. *Revista Bolivariana de derecho*, 2016, nº 21, 210-229.
- COLAS TURÉGANO, Asunción: Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter), en: GONZÁLEZ CUSSAC, José L. (dir.)/ MATALLÍN EVANGELIO, Ángela/ GORRIZ ROYO, Elena (coords.): *Comentarios a la reforma del Código Penal de 2015*, Tirant lo Blanch, Valencia, 2015, 663-681.

- CONCEPCIÓN OBISPO, Triana: Circular 3/2017, de 21 de septiembre, sobre la reforma del código penal operada por la LO 1/2015, de 30 de marzo en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos**.** *Revista Aranzadi Doctrinal*, 2017, nº 10, 183-192.
- CONTRERAS SOLER, Beatriz/GARRÓS FONT, Imma: Los principales delitos cibernéticos cuyos sujetos pasivos pueden ser los particulares, las personas jurídicas o la Administración Pública. *Revista de derecho y proceso penal*, 2017, nº 48, 133-148.
- DÍAZ GÓMEZ, Andrés: El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest, *REDUR*, 2010, 8, 169-203.
- FERNÁNDEZ BERMEJO, Daniel / MARTÍNEZ ATIENZA, Gorgonio: Ciberseguridad, ciberespacio y ciberdelincuencia, 1ª ed., Aranzadi, Cizur Menor (Navarra), 2018.
- GIL ANTÓN, Ana María: De los delitos contra la intimidad personal y familiar y delito informático, de acuerdo con la reforma operada por la lo 1/2015, de 30 de marzo, de reforma del Código Penal. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 2017, nº 39, 1-21.
- GONZÁLEZ COLLANTE, Tália: Los delitos contra la intimidad tras la reforma de 2015: luces y sombras. *Revista de derecho penal y criminología*, 2015, nº13, 51-83.
- GONZÁLEZ HURTADO, Jorge Alexandre: La seguridad en los sistemas de información como un bien jurídico de carácter autónomo. Perspectiva europea y española. *Revista Penal de México*, 2016, nº 9, 59-76.
- MAYER LUX, Laura: Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, 2018, nº 1, 159-206.
- RAMOS MOROCHO, Raúl Armando/ GALLEGOS MOSQUERA, Enrique: Infección con ransomware en el servidor de base de datos del sistema Onsystec ERP**.** *3c Tecnología: glosas de innovación aplicadas a la pyme,* 2016, nº 5, 56-76.
- ROMEO CASABONA, Carlos María: Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio, en: ROMEO CASABONA, Carlos María/ SOLA RECHE, Esteban/ BOLDOVA PASAMAR Miguel Ángel

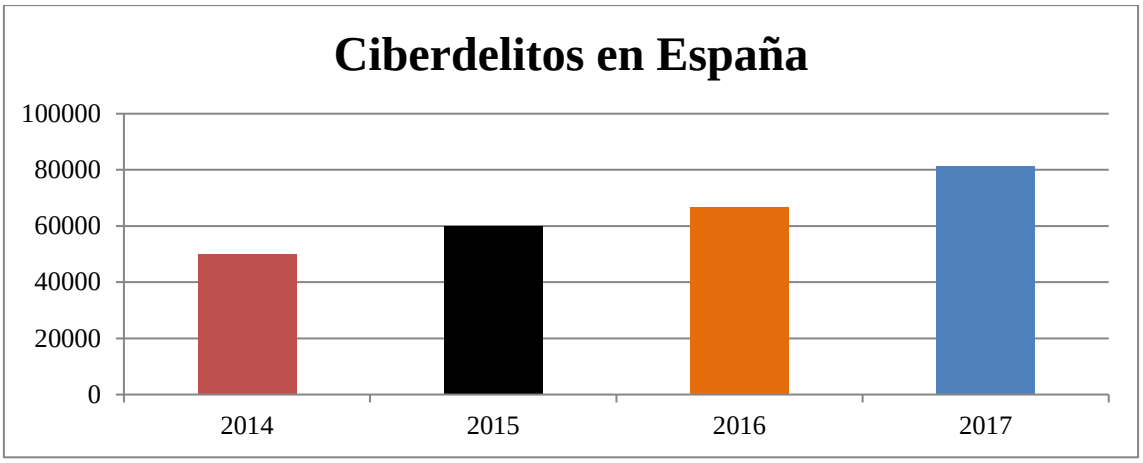
(coords.): *Derecho Penal. Parte Especial: Conforme a las Leyes Orgánicas 1 y 2/2015, de 30 de marzo*, Comares, Albolote (Granada), 2016, 254-285.

- 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, Juana (coord.): *Algunas cuestiones de parte especial tras la reforma del Código Penal*, Tirant lo Blanch, Valencia, 2018, 133-186.
- TOMÁS-VALIENTE LANUZA, Mª del Carmen: Delitos contra la intimidad y redes sociales (en especial, en la jurisprudencia más reciente). *Revista de Internet, Derecho y Política*, 2018, nº 27, 30-41.

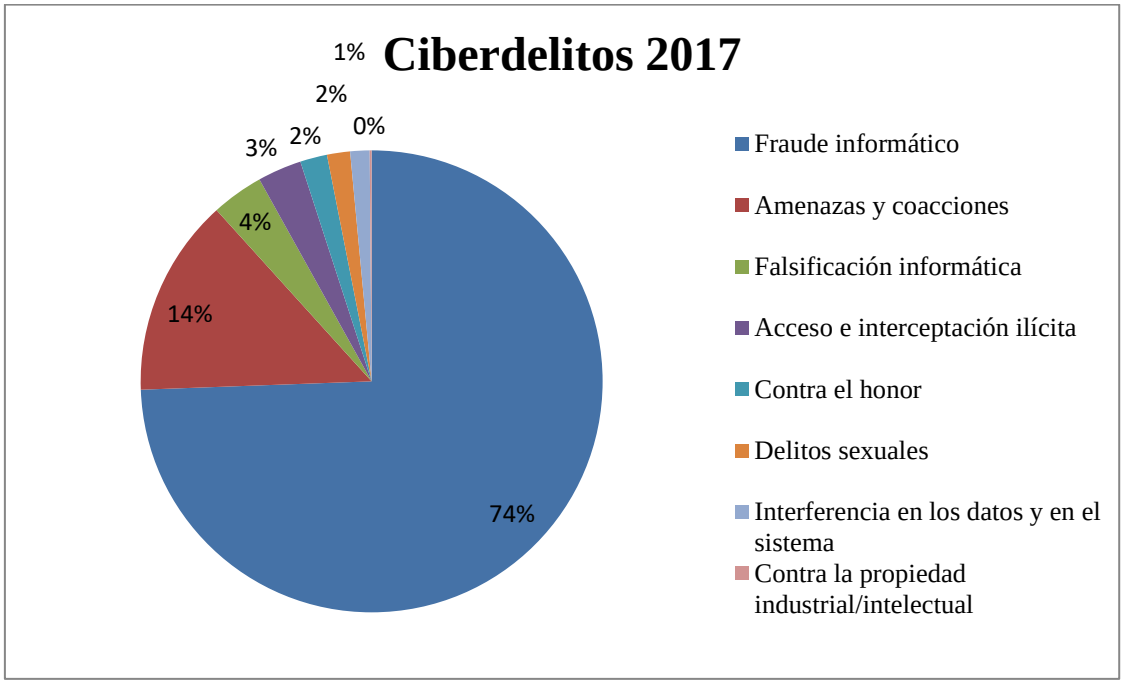
JURISPRUDENCIA

- STS, Sala de lo Penal, núm.1939/2013 de 3 de mayo.
- SAP de Vizcaya núm. 90307/2014 de 23 julio.
- SAP de Madrid núm. 6026/2015 de 27 de abril.
- SAP de Alicante núm. 3591/2015, de 16 de septiembre.
- STS, Sala de lo Penal, núm. 917/2016 de 2 de diciembre
- SAP de Madrid núm. 16438/2017, de 27 de noviembre.
- SAP de Madrid núm. 895/2017 de 27 noviembre.
- SAP de Pontevedra núm. 2823/2017 de 12 de diciembre.
- SAP de Madrid núm. 12606/2018 de 14 de septiembre.
- SAP de Lleida núm. 201/2018 de 4 mayo.
- SAP de Salamanca, núm. 37/2018 de 29 junio

ANEXOS



- **ANEXO 1**. Datos extraídos del OEDI. Disponible en http://oedi.es/estadisticas/. Visto el 7 de junio de 2019.



- **ANEXO 2**. Datos extraídos del OEDI. Disponible en http://oedi.es/estadisticas/. Visto el 8 de junio de 2019.