COLECCIÓN DE DERECHO DE LAS NUEVAS TECNOLOGÍAS

Directores:

GUILLERMO CERDEIRA BRAVO DE MANSILLA

Catedrático de Derecho civil de la Universidad de Sevilla

MIGUEL L. LACRUZ MANTECÓN

Profesor titular de Derecho civil de la Universidad de Zaragoza

EL MERCADO DIGITAL EN LA UNIÓN EUROPEA

Directores

Paula Castaños Castro

José Antonio Castillo Parrilla

Coordinadoras

Alicia María Pastor García

Isabel Luisa Martens Jiménez

AGUSTÍN MADRID PARRA
ALBERTO DE FRANCESCHI
TERESA RODRÍGUEZ DE LAS HERAS BALLELL
FRANCISCO PERTÍÑEZ VÍLCHEZ
SERGIO CÁMARA LAPUENTE
TATIANA ARROYO VENDRELL
FRANCISCA Mª ROSSELLÓ RUBERT
JOSÉ ANTONIO CASTILLO PARRILLA
JUDITH MORALES BARCELÓ
SEBASTIÁN LÓPEZ MAZA
GEMMA MINERO ALEJANDRE
PAULA CASTAÑOS CASTRO
JOAQUÍN JOSÉ NOVAL LAMAS
JUAN FRANCISCO RODRÍGUEZ AYUSO
MARÍA DOLORES ORTIZ VIDAL
RUBÉN LÓPEZ PICÓ
JUAN JESÚS MARTOS GARCÍA
JOSÉ MIGUEL MARTÍN RODRÍGUEZ
JUAN CALVO VÉRGEZ
JOSÉ MANUEL MACARRO OSUNA
GUILLERMO SÁNCHEZ-ARCHIDONA HIDALGO
Mª DEL MAR SOTO MOYA
JAVIER VALLS PRIETO
CARMEN ROCÍO FERNÁNDEZ DÍAZ
JAVIER GÓMEZ LANZ
MYRIAM CABRERA MARTÍN
ANTONINO DI MAIO
MARTA FERNÁNDEZ CABRERA
REMEDIOS CAMPOY GÓMEZ
ANTONIO MERCHÁN MURILLO
ALBA PAÑOS PÉREZ
MARÍA JESÚS BLANCO SÁNCHEZ
ENRIQUE MORENO SERRANO

REUS

EDITORIAL

Madrid, 2019

C/ Rafael Calvo, 18, 2º C – 28010 Madrid
+34 91 521 36 19 – +34 91 522 30 54
reus@editorialreus.es
www.editorialreus.es

1.ª edición REUS, S.A. (2019)
ISBN: 978-84-290-2116-5
Depósito Legal: M-4047-2019
Diseño de portada: María Lapor
Impreso en España
Printed in Spain

Imprime: Ulzama Digital

CAPÍTULO 23: LOS DELITOS INFORMÁTICOS EN EL MERCADO DIGITAL: APUNTES PENALES Y CRIMINOLÓGICOS, por CARMEN ROCÍO FERNÁNDEZ DÍAZ 535
I. Introducción 535
II. Los delitos informáticos en el mercado digital de la Unión Europea 537
III. Aspectos penales 538
III.1. Conductas típicas de los delitos informáticos 538
III.2. El tipo subjetivo de los delitos informáticos 540
III.3. Consecuencias penológicas de los delitos informáticos 541
IV. Aspectos criminológicos 543
V. Conclusiones 544
VI. Bibliografía 546

CAPÍTULO 24: CREACIÓN DEL MERCADO ÚNICO DIGITAL Y COMISIÓN DE DELITOS PUBLICITARIOS A TRAVÉS DE LA WEB, por JAVIER GÓMEZ LANZ 547
I. Introducción 547
II. El artículo 282 del Código Penal como medio diferenciado de tutela penal de los derechos de los consumidores en el entorno digital 549
III. Valoración político-criminal del 282 CP: ¿es necesaria una respuesta adicional del ordenamiento español para garantizar la credibilidad del mercado digital? 552
IV. Bibliografía 559

CAPÍTULO 25: ALGUNAS CUESTIONES RELEVANTES SOBRE LA REGULACIÓN EN MATERIA DE CONTENIDOS ILÍCITOS EN LÍNEA, por MYRIAM CABRERA MARTÍN 561
I. La lucha contra los contenidos ilícitos en la Estrategia para el Mercado Único Digital en Europa 561
II. Tratamiento de los contenidos ilícitos en nuestra legislación penal a la luz de las directrices europeas sobre la materia 563
II.1. Pornografía infantil 564
II.2. Terrorismo 566
II.3. Discurso del odio 567
III. Responsabilidad de los proveedores de servicios de alojamiento de datos 569
IV. Bibliografía 573

CAPÍTULO 26: PHISHING E MERCATO DIGITALE, TRA NUOVI RISCHI PER I CONSUMATORI E RECENTI RIFLESSIONI PENALISTICHE, por ANTONINO DI MAIO 575

CAPÍTULO 23

LOS DELITOS INFORMÁTICOS EN EL MERCADO DIGITAL: APUNTES PENALES Y CRIMINOLÓGICOS[1]

CARMEN ROCÍO FERNÁNDEZ DÍAZ
Doctora en Derecho y Profesora de Derecho penal y Criminología
Universidad de Málaga

Sumario: I. Introducción. II. Los delitos informáticos en el mercado digital de la Unión Europea. III. Aspectos penales. III.1. Conductas típicas de los delitos informáticos. III.2. El tipo subjetivo de los delitos informáticos. III.3. Consecuencias penológicas de los delitos informáticos. IV. Aspectos criminológicos. V. Conclusiones. VI. Bibliografía.

I. INTRODUCCIÓN

La información se ha convertido en las últimas décadas en un bien de incalculable valor para las personas, tanto físicas como jurídicas. La gravedad de los ataques a la información viene dada por la multitud de bienes jurídicos a los que aquellos afectan. La intimidad, el patrimonio, la libertad sexual, la seguridad nacional, o la propiedad intelectual e industrial son solo algunos de

[1] Este trabajo ha sido realizado en el marco del Proyecto de Investigación titulado "La Estrategia para el Mercado Único Digital Europeo y sus consecuencias jurídico privadas, tributarias y penales", financiado por el I Plan Propio de Investigación y Transferencia de la Universidad de Málaga, del que la autora forma parte como investigadora.

los objetos de tutela cuya violación puede producirse a partir de un ataque a sistemas de información que contengan datos relacionados con estos bienes.

Como bien de naturaleza intangible, las formas de ataque a la información resultan cada vez más complejas y su perpetración cada vez más habitual, por lo que su protección constituye hoy en día un objetivo de primer orden para la Unión Europea y para sus Estados miembros. No hay más que acceder a cualquier diario de noticias para ver con qué frecuencia se suceden incidentes relativos a ataques de información. Sin embargo, uno de los sectores en los que mayores efectos perjudiciales genera la ciberdelincuencia es en el ámbito empresarial. El Mercado Digital constituye el escenario idóneo para generar perjuicios a los agentes económicos que intervienen en él y para obtener beneficios de forma fraudulenta, pues además de lo anterior, en gran parte de los supuestos los usuarios ignoran estar siendo víctimas de un ataque. Así, en el Estudio sobre la Ciberseguridad y confianza en los hogares españoles, publicado en mayo de 2018 por el Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información, un 61,7% de los usuarios encuestados que declararon no tener un virus en sus ordenadores, en realidad lo tenían (ONTSI, 2018, p. 35)[2].

Lo anterior demuestra la necesidad de tomar conciencia sobre este fenómeno que puede afectar de manera grave a diversos intereses de los ciudadanos, pero que donde mayor caldo de cultivo encuentra, como veremos, es en los de carácter económico. Por ello, en el presente trabajo se abordará, en primer lugar, cuáles han sido algunas de las medidas que desde la Unión Europea se han adoptado para luchar contra los ataques a la ciberseguridad. En segundo lugar, se estudiará la regulación de algunos de los aspectos penales más destacados, como son las conductas típicas, el tipo subjetivo de estas figuras delictivas y sus consecuencias penológicas. Y, en tercer lugar, se aportarán algunos datos relativos a este fenómeno delictivo para poner de manifiesto cuál es la situación actual en España respecto a la ciberdelincuencia y, en concreto, a los delitos informáticos.

[2] ONTSI (Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información): *Estudio sobre la Ciberseguridad y confianza en los hogares españoles*, mayo 2018, p. 35. Estudio accesible a través del siguiente enlace: http://www.ontsi.red.es/ontsi/sites/ontsi/files/Ciberseguridad%20y%20Confianza%20en%20los%20hogares%20espa%C3%B1oles%20%28mayo%202018%29.pdf.

II. LOS DELITOS INFORMÁTICOS EN EL MERCADO DIGITAL DE LA UNIÓN EUROPEA

Como ya ha sido apuntado, la ciberseguridad constituye uno de los principales objetivos sobre los que existe preocupación a nivel europeo. La consecución de una economía competitiva, que esté basada en la innovación como elemento clave para el buen funcionamiento del mercado interior europeo sin barreras fronterizas requiere de la creación de un entorno digital seguro, en el que las empresas puedan ofrecer sus bienes y servicios sin temer posibles intromisiones ilegítimas externas y los consumidores puedan adquirirlos con total confianza.

Por ello, esta preocupación ha llevado ya desde hace casi dos décadas a tomar medidas desde la Unión para que sus Estados Miembros reaccionen ante estas amenazas. La primera piedra en este ámbito se puso con el llamado "Convenio Budapest", esto es, con el *Convenio sobre Ciberseguridad*, celebrado en dicha ciudad el 23 de noviembre de 2001 y ratificado por España en septiembre de 2010[3]. Desde entonces han sido numerosos los textos que han ido conformando un marco jurídico de referencia para la lucha contra la cibercriminalidad, cristalizando en importantes estrategias e instrumentos normativos internacionales de gran repercusión en las legislaciones nacionales.

Así, los últimos textos a nivel europeo, y a los que se hará especial referencia en la presente investigación, son, por un lado, 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*[4], que sustituye a la Decisión Marco 2005/222/JAI del Consejo, ya mencionada y cuyo objetivo es establecer normas mínimas relativas a la definición de las infracciones penales y las sanciones aplicables para aproximar las normas penales de los Estados miembros en materia de ataques contra los sistemas de información y mejorar la cooperación entre las autoridades competentes. Y, por otro lado, la *Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión*[5]. Esta Directiva, de aplicación exclusiva a las administraciones públicas que hayan sido identificadas como operadores de servicios esenciales, incluye un anexo con estos últimos en el que se encuentran la energía, el transporte, la banca, las infraestructuras de los mercados financieros, el sector sanitario, el suministro y distribución de agua potable y la infraestructura digital.

---

3 Al instrumento de ratificación puede accederse a través del siguiente enlace: https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf.

4 Diario Oficial de la Unión Europea L 218/8, 14.8.2013.

5 Diario Oficial de la Unión Europea L 194/1, 19.7.2016.

En este contexto, el legislador español ha ido haciéndose eco en los últimos años de las directrices marcadas por Europa y ha ido modificando la regulación penal de determinadas cuestiones relacionadas con el mercado y con la ciberdelincuencia, en especial, en lo que respecta a los delitos informáticos.

III. ASPECTOS PENALES

El legislador penal ha ido adaptando la normativa penal española a las directrices marcadas por la Unión Europea. Así, la LO 5/2010, de 22 de junio, dio respuesta en su momento a la ya derogada Decisión Marco 2005/222/JAI, de 24 de febrero de 2005, mientras que la reforma llevada a cabo por la LO 1/2015, de 30 de marzo, se ocupó especialmente de la transposición de la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información y la interceptación de datos electrónicos cuando no se trata de una comunicación personal.

De esta forma, los delitos informáticos han sufrido modificaciones en los últimos años, siendo de especial relevancia aquellas a las que haremos mención, que tienen que ver con las conductas típicas, el tipo subjetivo y las consecuencias penológicas.

III.1. Conductas típicas de los delitos informáticos

En primer lugar, hay que mencionar la conducta de *acceso ilegal a un sistema informático*. La Directiva 2013/40/UE, en su artículo 3, resta discrecionalidad a los legisladores nacionales al establecer los límites del acceso ilícito obligando a que se dé una violación de una medida de seguridad para que aquella constituya delito. Este requisito tenía carácter facultativo, aunque España ya lo había introducido antes de la reforma de 2015. De esta forma, la presente regulación exige el sorteo ilícito de las barreras impuestas por el titular de sistemas de información, con el fin de protegerlos, lo que parece acorde al principio de intervención mínima.

Así, a partir de la reforma de 2015 se introdujo en el Código penal también una regulación autónoma del delito de intrusión informática o "*hacking*", previendo el artículo 197 bis CP una pena de prisión de seis meses a dos años al que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o se lo facilite a otro (novedad de la reforma), al conjunto o a una parte de un sistema de información o se mantenga en él contra la voluntad de quien

tenga el legítimo derecho a excluirlo. El castigo de esta conducta pretende tutelar la privacidad, como bien jurídico diferenciado de la intimidad[6].

En segundo lugar, hay que aludir a la *interferencia ilegal en los sistemas informáticos*, es decir, el llamado "sabotaje informático", previsto en el artículo 4 de la Directiva de 2013 y en el artículo 264 bis del CP. Este último castiga con pena de prisión de seis meses a tres años al que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, lo cual puede tener lugar de alguna de las siguientes formas: a) realizando alguna de las conductas a las que se refiere el artículo 264 CP, es decir, borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Con esta regulación se dotó a este delito de autonomía y se previeron de forma tasada sus medios comisivos, mejorando así su técnica legislativa.

En tercer lugar, hay que hacer referencia a la *interferencia ilegal en los datos*, con conductas como "...borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos contenidos en un sistema de información, intencionalmente y sin autorización", según el artículo 5 de la Directiva. El legislador español de 2015 no hizo sustanciales modificaciones en esta figura delictiva, prevista en el artículo 264.1 CP, más allá de aumentar el límite máximo del marco penal en un año.

En cuarto lugar, se prevé la conducta de *interceptación ilegal* en el artículo 6 de la Directiva, que debe ser sancionada, en los casos que no sean de menor gravedad, cuando esta conducta se cometa "...por medios técnicos, de transmisiones no públicas de datos informáticos hacia, desde o dentro de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos informáticos, intencionalmente y sin autorización...". La regulación española de este delito, recogida en el artículo 197 bis 2 CP y que prevé una pena de prisión de tres meses a dos años o multa de tres a doce meses, es fiel a la literalidad de la Directiva,

[6] Así, el propio Preámbulo de la Ley, en su apartado XIII, puso de manifiesto que para transponer la Directiva 2013/40/UE, de 12 de agosto, relativa a los ataques contra los sistemas de información, era necesario distinguir los supuestos de revelación de datos que afectaban directamente a la intimidad personal, del acceso a otros datos o informaciones que podían afectar más bien a la privacidad, pero que no estaban referidos directamente a la intimidad personal. También en este sentido, en el ordenamiento jurídico italiano, PICOTTI, L.: "Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale", en *Diritto dell'internet*, n.2/2005, p. 193; el mismo: "Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati", en PICOTTI, L. (Dir.): *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, Padova, 2004, pp. 80 y ss.

salvo porque obvia el elemento de la intencionalidad, a mi juicio, por su evidente exigencia a pesar de no estar presente en la figura delictiva, ya que en realidad equivaldría al dolo de realizar los elementos objetivos del tipo.

En quinto lugar, hay que mencionar la *puesta a disposición de instrumentos para cometer las citadas infracciones*, prevista en el artículo 7 de la Directiva, y entendida como "...la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición" de (a) "un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6" o de (b) "una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información". El legislador español de 2015 introdujo esta infracción para los delitos informáticos (artículo 197 ter CP) y para los daños (artículo 264 ter CP), respetando también el tenor literal de lo previsto en la Directiva, aunque con mayor claridad expositiva, y siendo las conductas que recoge consideradas por algún autor como constitutivas de actos preparatorios de estos delitos (MUÑOZ CONDE, 2015, p. 416)[7]. La punición de actos preparatorios mediante su tipificación en relación con las nuevas tecnologías, ampliando así la descripción típica a fin de cubrir lagunas de punibilidad, parece ser un rasgo común de los delitos relacionados con aquellas (FARALDO CABANA, 2016).

Y, en sexto lugar, otro tipo de conductas que la Directiva considera necesario castigar, en este caso mediante una circunstancia agravante para una lucha integrada contra la ciberdelincuencia, son las *usurpaciones de identidad e infracciones relacionadas*. Con este fin, la reforma de 2015 introdujo en los delitos de daños o sabotaje de datos (artículo 264.3 CP) y sistemas informáticos (artículo 264 bis 3 CP), idéntica redacción para castigar con las penas previstas en los apartados anteriores correspondientes en cada caso, en su mitad superior, a quienes hubieren cometido los hechos "...mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero".

III.2. El tipo subjetivo de los delitos informáticos

La Directiva de 2013, en su Considerando (17), introdujo también una disposición en la que tiene especialmente en cuenta los principios básicos del Derecho penal y el concepto personal de lo injusto. Partiendo de dichos parámetros, la Directiva prevé que no se establecerán responsabilidades penales

[7] En el mismo sentido se pronuncia MUÑOZ CONDE, F.: *Derecho penal. Parte especial*, 20ª edición, completamente revisada y puesta al día conforme a las Leyes Orgánicas 1/2015 y 2/2015, de 30 de marzo, Tirant lo Blanch, Valencia, 2015, p. 416.

cuando, cumpliéndose los criterios objetivos de las infracciones que recoge, los actos se cometan sin propósito delictivo. Algunos posibles ejemplos a los que alude son, entre otros, que la persona no supiera que el acceso no estaba autorizado o que una empresa o un vendedor designen a una persona para probar la solidez de su sistema de seguridad.

Para garantizar esta previsión, la Directiva exige para cada una de sus infracciones que estas se cometan intencionalmente y sin autorización. A mi juicio, la referencia a la intención no es más que el dolo de realizar los elementos objetivos del tipo, mientras que la exigencia de que la conducta se realice sin autorización es un elemento que se materializa en el tipo en la necesidad de que se vulneren las medidas de seguridad impuestas por el titular de los datos o sistemas de información[8].

III.3. Consecuencias penológicas de los delitos informáticos

Teniendo en cuenta que la Directiva tiene efectos jurídico-penales en los ordenamientos jurídicos de los Estados Miembros, esta también se pronuncia sobre las sanciones a imponer respecto de las infracciones que prevé.

Así, en su artículo 9 establece que dichas sanciones deben ser penas efectivas, proporcionadas y disuasorias, y en su apartado 2 establece sanciones mínimas para las infracciones previstas en los artículos 3 a 7, que deberán castigarse con una sanción máxima de privación de libertad igual o superior a dos años, en los casos que no sean de menor gravedad.

Con dicho límite impuesto por la normativa europea, el legislador español, por un lado, mantiene exactamente este límite máximo en el caso del acceso ilegal a los sistemas de información, la interceptación ilegal y la puesta a disposición de instrumentos para cometer las citadas infracciones, previendo además en estos dos últimos delitos la pena de multa como alternativa a la prisión. Por otro lado, en los delitos de interferencia ilegal en los sistemas de información y en los datos, el legislador de 2015 decidió homogeneizar las penas, elevando el límite máximo del marco penal del segundo de los delitos, de dos a tres años y equiparando con dicha modificación ambas conductas, lo que resulta inoportuno, a mi juicio, dada su diversa gravedad.

---

[8] Una opinión diferente en relación al elemento que exige la falta de autorización es la que defiende MARTÍNEZ-BUJÁN PÉREZ, C.: *Delitos relativos al secreto de empresa*, Tirant Lo Blanch, Valencia, 2010, p. 46 nota 67, quien estima en relación al delito de espionaje empresarial en el ordenamiento jurídico alemán, que exige este elemento, que se trata de uno con carácter implícito en este tipo de comportamientos delictivos, pues en aquellos casos en los que un sujeto estuviera autorizado por el titular de los datos o sistemas informáticos o por el Derecho a acceder a ellos, interceptarlos o interferir en ellos, no se daría ninguna de estas infracciones.

Por último, el artículo 9 de la Directiva establece también en sus apartados 3 y 4 sanciones agravadas en determinados supuestos, referidos exclusivamente a las conductas de interferencia ilegal en sistemas de información y en datos o programas informáticos o documentos electrónicos (artículos 4 y 5). De estas exigencias internacionales se ha hecho eco el legislador español tanto en lo que respecta al delito de daños como a los relativos a la intimidad. Sin embargo, en algunos casos este se ha excedido de dichas exigencias, castigando duramente estos supuestos, al optar en la mayoría de las figuras por la pena máxima de cinco años, para casos en los que la Directiva exige al menos tres (como ocurre en las figuras previstas en los artículo 264.2.2ª y 5ª, 264 bis y 264 ter CP) o incluso ocho años (como es el caso del artículo 264 bis 2 CP). De este modo, el texto español resulta ser incluso más punitivo que la propia Directiva (De la Mata Barranco, 2017, p. 238).

La única vía que deja el legislador en estos casos a una menor punición es la discrecionalidad judicial que queda en la determinación de cuándo los daños son considerados graves (Castro Corredoira / Vázquez-Portomeñe Sijas, 2015, p. 832)[9] o qué se entiende por un número significativo de sistemas de información. No hay que obviar tampoco que en estos casos, recogidos en los artículos 264.2.3ª CP y 264 bis 2 CP, la pena de multa proporcional prevista, especialmente elevada por lo demás, no es alternativa a la privativa de libertad, sino acumulativa a esta y, por tanto, de obligada imposición, por lo que es de destacar la especial gravosidad de estas penas, que no solo privan de libertad por largo tiempo en muchos casos, sino también de parte del patrimonio del sujeto condenado a ellas.

En definitiva, parece que cabe preguntarse aquí, dejando la cuestión en el aire por tener entidad suficiente para constituir una nueva investigación y de acuerdo con la reflexión que hace De la Mata Barranco, "hasta qué punto la actuación de la Unión puede quebrar el principio de proporcionalidad de las normas penales (...) exigiendo determinados máximos penales (...) y hasta qué punto se puede obligar a la sanción de determinadas conductas (...) que no encuentran siempre paralelo en otros campos delictivos" (De la Mata Barranco, 2017, pp. 240-241).

[9] Al no haber previsto el legislador criterio alguno para valorar la relevancia del perjuicio causado a la actividad empresarial o cuándo los daños ocasionados son considerados graves, ello debería determinarse en el caso concreto. En el mismo sentido, Castro Corredoira, M. / Vázquez-Portomeñe Seijas, F.: "La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP", en González Cussac, J. L. (Director), *Comentarios a la reforma del Código penal de 2015*, 2ª edición, Tirant lo Blanch, Valencia, 2015, p. 832, quienes afirman que ello deja la puerta abierta al arbitrio judicial.

IV. ASPECTOS CRIMINOLÓGICOS

La situación actual de España en lo que respecta a la perpetración de delitos informáticos no parece ir en consonancia con los esfuerzos que se hacen desde el ámbito legislativo penal, en cumplimiento con las directrices impuestas desde la Unión Europea, en la lucha contra la ciberdelincuencia en general, y los delitos informáticos, en particular.

Así, por un lado, Europol ha publicado recientemente un informe, el IOCTA 2017, por sus siglas en inglés "*Internet Organised Crime Threat Assessment*", en el que pone de manifiesto que España ocupa la posición número cinco en Europa con mayor número de detecciones de ataques a través de ciertos tipos de virus informáticos, como son el *malware* y los *botnets*[10]. Junto a estas dos tipologías de ataques informáticos, en mayo de 2017 tuvo lugar un ataque global de *ransomware* sin precedentes, el llamado virus *WannaCry*, que se cree que afectó gravemente a más de 300.000 víctimas en 150 países, incluido el servicio de telecomunicaciones de *Telefónica* en España.

Los datos que el Ministerio del Interior ofrece sobre los delitos informáticos muestran también un incremento de estos en los últimos años. Así, en el año 2017 aumentó el número de este tipo de delitos detectados en un 22,1% respecto al año anterior, correspondiendo el 74,4% de esta cifra a fraudes informáticos, es decir, un total de 60.511 hechos conocidos, duplicando así casi los 32.842 de 2014 (Ministerio del Interior, 2017, pp. 33 y 38)[11].

Además de lo anterior, el resumen ejecutivo del Centro Criptológico Nacional (CCN-CERT IA-16/17)[12] pone de relieve que el ciberespionaje económico constituye la principal amenaza para el mundo occidental y que este experimentó un importante crecimiento en 2016.

Estos datos ponen de manifiesto que figuras delictivas llevadas a cabo a través de medios tecnológicos y cuya comisión afecta especialmente al mercado presentan un crecimiento exponencial.

Por otro lado, hay que recordar lo que ya se mencionó al principio de este trabajo, y es que, según el Estudio sobre la Ciberseguridad y confianza en los hogares españoles, publicado en mayo de 2018 por el Observatorio Nacional

---

[10] EUROPOL: "Internet Organised Crime Threat Assessment – IOCTA 2017", *European Cybercrime Centre (EC3)*, 2017, p. 24.

[11] MINISTERIO DEL INTERIOR: *Estudio sobre la Cibercriminalidad en España*, 2017, pp. 33 y 38. Puede consultarse en el siguiente enlace: http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

[12] Puede accederse al citado documento en el siguiente enlace: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2221-ccn-cert-ia-16-17-ciberamenzas-y-tendencias-edicion-2017-resumen-ejecutivo-1.html.

de Telecomunicaciones y de la Sociedad de la Información, un 61,7% de los usuarios encuestados que declararon no tener un virus en sus ordenadores, en realidad lo tenían (ONTSI, 2018, p. 35)[13]. A lo anterior se suma que, según datos del Instituto Nacional de Estadística, desde el año 2008 el comercio electrónico se ha triplicado, al haber afirmado el 40% de las personas encuestadas en el año 2017 que han realizado alguna compra empleando las nuevas tecnologías, frente al 12,8% que lo hicieron en el año 2008[14].

Todo lo anteriormente expuesto lleva a concluir que, más que invertir los esfuerzos respecto a la lucha contra este tipo de criminalidad en el incremento de penas y las reformas penales de estas figuras delictivas, sería deseable prestar una mayor atención a la prevención de estos ataques. La doctrina más autorizada ha puesto de manifiesto que la autoprotección, de naturaleza preventiva, junto con las sanciones informales impuestas por las agencias encargadas de mantener el orden en la red, tienen un efecto mucho mayor sobre la delincuencia informática que cualquier reforma legislativa que se pueda implementar (FARALDO CABANA, 2016). Por ello, cuestión fundamental es la ciberseguridad y la protección blindada de nuestra información de toda naturaleza, especialmente la de carácter económico, de forma que esta no se descuide, pues tratándose de un bien inmaterial, los ataques a esta también lo son, y siendo por ello prácticamente imperceptibles, resulta fundamental adoptar las medidas necesarias para, en lo posible, poder evitarlos.

V. CONCLUSIONES

La ciberseguridad constituye uno de los objetivos de primer orden de la Unión Europea y su importancia se extiende a los Estados miembros para que estos adopten las medidas legales necesarias para su efectiva consecución. Con dicho fin, el legislador español otorga una protección plena a los sistemas de información y a los datos, programas y documentos contenidos en ellos, castigando las conductas constitutivas de los delitos informáticos.

---

[13] ONTSI (Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información): *Estudio sobre la Ciberseguridad y confianza en los hogares españoles*, mayo 2018, p. 35. Estudio accesible a través del siguiente enlace: http://www.ontsi.red.es/ontsi/sites/ontsi/files/Ciberseguridad%20y%20Confianza%20en%20los%20hogares%20espa%C3%B1oles%20%28mayo%202018%29.pdf.

[14] Datos del Instituto Nacional de Estadística (INE), sistematizados en el *Estudio sobre la Cibercriminalidad en España*, 2017 del Ministerio del Interior, p. 20. Puede consultarse en el siguiente enlace: http://www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Por un lado, en relación a las cuestiones de índole penal, la regulación de estas figuras delictivas ha ido modificándose tras los cambios legislativos que se han sucedido en Europa. Así, en lo que respecta a las conductas típicas, la regulación de estos delitos, con carácter previo a la reforma de 2015 ya castigaba comportamientos como el acceso a sistemas informáticos, la interferencia ilegal en datos y sistemas o la interceptación de las telecomunicaciones para descubrir los secretos relativos a la intimidad o pertenecientes a la empresa. La reforma de 2015 vino a ampliar notablemente estas conductas, introduciendo otras que antes podían considerarse como participación —como la de facilitar el acceso ilegal a un tercero a un sistema de información—, o como actos preparatorios —como es la puesta a disposición de instrumentos para cometer las infracciones relacionadas con ataques a sistemas de información—. También introdujo la interceptación ilegal de transmisiones de datos informáticos desde, hacia o dentro de sistemas de información, complementando las ya existentes interceptaciones de las telecomunicaciones y castigando con la mitad superior de la pena en cuestión de los delitos de daños a datos o a sistemas, las usurpaciones de identidad en este ámbito. En relación con las sanciones, a mi juicio, el legislador español va mucho más allá de lo exigido por la normativa europea, imponiendo penas de dos años de prisión para actos meramente preparatorios y otras que, en algunos casos, son muy superiores a las previstas en la Directiva de 2013, como son los supuestos en los que esta requiere una sanción máxima de al menos tres años de prisión y la regulación española llega a prever algunas de hasta ocho años. En mi opinión, habría sido deseable, además, un mayor uso de la pena de multa, ausente en supuestos en los que resultaría adecuada su aplicación, como es el caso del tipo básico de daños informáticos a datos (artículo 264.1 CP) o el de acceso ilegal a sistemas de información (artículo 197 bis CP), cuya pena única es la prisión.

Por otro lado, ha podido constatarse que este incremento punitivo no se corresponde con un descenso de este tipo de criminalidad, sino más bien todo lo contrario. Grandes empresas de nuestro país, como es el caso de Telefónica, sufren ataques a sus sistemas informáticos y delitos como el ciberespionaje empresarial constituyen importantes amenazas al patrimonio de las empresas españolas. A ello se suma la invisibilidad de estos ataques y el cada vez mayor uso de las nuevas tecnologías en el mercado digital por parte de la ciudadanía.

Todo lo anterior lleva a concluir que, más que seguir invirtiendo esfuerzos en llevar a cabo reformas legislativas desde el Derecho penal con un mayor incremento de las penas aplicables a estos delitos, hay que poner el foco de atención en la necesidad de adoptar medidas preventivas que permitan implementar un sistema eficaz de seguridad cibernética, de forma que los ataques puedan evitarse en lugar de seguir endureciendo la reacción penal a los mismos.

VI. BIBLIOGRAFÍA

CASTRO CORREDOIRA, M. / VÁZQUEZ-PORTOMEÑE SEIJAS, F. (2015). "La reforma de los delitos de daños: arts. 263, 264, 264 bis, 264 ter, 264 quáter, 265, 266.1 y 266.2 CP", en GONZÁLEZ CUSSAC, J. L. (Director), *Comentarios a la reforma del Código penal de 2015*, 2ª edición, Tirant lo Blanch, Valencia.

DE LA MATA BARRANCO, N. (2017). "Capítulo VI. Delitos informáticos (contra sistemas y datos)", en DE LA CUESTA ARZAMENDI (Dir.) / DE LA MATA BARRANCO, N. (Coord.): *Adaptación del derecho penal español a la política criminal de la Unión Europea*, Thomson Reuters Aranzadi, Pamplona, pp. 221-243.

EUROPOL (2017). "Internet Organised Crime Threat Assessment – IOCTA 2017", *European Cybercrime Centre (EC3)*.

FARALDO CABANA, P. (2016). "Estrategias legislativas en las reformas de los delitos informáticos contra el patrimonio", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Número 42 (septiembre - diciembre).

MARTÍNEZ-BUJÁN PÉREZ, C. (2010). *Delitos relativos al secreto de empresa*, Tirant Lo Blanch, Valencia.

MINISTERIO DEL INTERIOR (2017). *Estudio sobre la Cibercriminalidad en España*.

MUÑOZ CONDE, F. (2015). *Derecho penal. Parte especial*, 20ª edición, completamente revisada y puesta al día conforme a las Leyes Orgánicas 1/2015 y 2/2015, de 30 de marzo, Tirant lo Blanch, Valencia.

ONTSI (MAYO 2018). (Observatorio Nacional de Telecomunicaciones y de la Sociedad de la Información): *Estudio sobre la Ciberseguridad y confianza en los hogares españoles*.

PICOTTI, L. (DIR.). (2004). *Il diritto penale dell'informatica nell'epoca di Internet*, CEDAM, Padova.

PICOTTI, L. (2005). "Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale", en *Diritto dell'internet*, n.2.