Carlos María Romeo Casabona
M.ª Ángeles Rueda Martín (*Eds.*)

Derecho Penal, ciberseguridad, ciberdelitos e inteligencia artificial

Volumen I: Ciberseguridad y ciberdelitos

EDITORIAL COMARES

ESTUDIOS DE DERECHO PENAL
Y CRIMINOLOGÍA
dirigidos por
Carlos María Romeo Casabona

Carlos María Romeo Casabona
M.ª Ángeles Rueda Martín
Editores

DERECHO PENAL, CIBERSEGURIDAD, CIBERDELITOS E INTELIGENCIA ARTIFICIAL

Volumen I
Ciberseguridad y ciberdelitos

Granada, 2023

BIBLIOTECA COMARES DE CIENCIA JURÍDICA

ESTUDIOS DE DERECHO PENAL
Y CRIMINOLOGÍA
dirigidos por
Carlos María Romeo Casabona
143

Editorial Comares, 2023
Polígono Juncaril
C/ Baza, parcela 208
18220 Albolote (Granada)
Tlf.: 958 465 382

http://www.editorialcomares.com • E-mail: libreriacomares@comares.com
https://www.facebook.com/Comares • https://twitter.com/comareseditor
https://www.instagram.com/editorialcomares

ISBN: 978-84-1369-670-6 • Depósito legal: 1646/2023

Fotocomposición, impresión y encuadernación: Comares

En permanente recuerdo del Maestro don José Cerezo Mir

SUMARIO

Capítulo 2
AMENAZAS COMPLEJAS EN EL CIBERESPACIO, ESTADO DEL ARTE Y PROSPECTIVA
Luis Fernando Hernández García

Capítulo 3
EL CIBERESPACIO COMO NUEVO ESCENARIO PARA VULNERAR DERECHOS FUNDAMENTALES
Aitziber Emaldi Cirión

Capítulo 4
LA INTROMISIÓN DEL DERECHO PENAL EN LA PROTECCIÓN DE LA CIBERSEGURIDAD

Esteban Sola Reche

Capítulo 5
ALGUNAS REFLEXIONES JURÍDICAS SOBRE LOS DELITOS DEL SIGLO XXI: CIBERCRIMEN, INTERNET OSCURA Y Covid-19

Elena Atienza Macías
Silvia Irene Verdugo Guzmán

Capítulo 6

EL PROTOCOLO ADICIONAL AL CONVENIO SOBRE CIBERDELINCUENCIA COMO RESPUESTA INTEGRADORA ANTE LAS DIFICULTADES EN LA ATRIBUCIÓN DE LA JURISDICCIÓN PENAL

Ekain Payán Ellacuria

SEGUNDA PARTE

LOS CIBERDELITOS EN EL CÓDIGO PENAL ESPAÑOL

Capítulo 7

LA RESPUESTA DEL DERECHO PENAL ESPAÑOL ANTE LOS ATAQUES CONTRA LOS SISTEMAS DE INFORMACIÓN. UN ANÁLISIS CRÍTICO

Aliuska Duardo Sánchez

Capítulo 8

ANÁLISIS JURISPRUDENCIAL DE LOS DELITOS CONTRA DATOS RESERVADOS DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD

Carlos Trincado Castán

Capítulo 9

EL DELITO DE INTRUSIÓN EN UN SISTEMA DE INFORMACIÓN

Carlos María Romeo Casabona

Capítulo 10
EL DELITO DE DAÑOS INFORMÁTICOS ANTE NUEVOS ESCENARIOS TECNOLÓGICOS
Pilar Nicolás

Capítulo 11
LOS ATAQUES DE DENEGACIÓN DE SERVICIOS COMO CIBERDELITO EN EL CÓDIGO PENAL ESPAÑOL
M.ª Ángeles Rueda Martín

Capítulo 13
LA APLICACIÓN DE LOS DELITOS CONTRA LOS SISTEMAS DE INFORMACIÓN POR LOS TRIBUNALES ESPAÑOLES

Carlos Trincado Castán

Capítulo 14
RESPUESTA PENAL A LA SUPLANTACIÓN DE IDENTIDAD. ESPECIAL CONSIDERACIÓN A LOS FRAUDES DE IDENTIDAD DIGITAL

Fátima Flores Mendoza

Capítulo 15
LA PROPORCIONALIDAD DE LA RESPUESTA PENAL AL CIBERESPIONAJE INDUSTRIAL Y AL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS POR MEDIO DE LA RED

Emilio José Armaza Armaza
Jon López Gorostidi

Capítulo 16
LA RESPUESTA JURÍDICA DEL CÓDIGO PENAL ESPAÑOL A LOS CIBERDELITOS COMETIDOS EN EL ÁMBITO DE ORGANIZACIONES O GRUPOS CRIMINALES

Miguel Ángel Boldova Pasamar

ABREVIATURAS

AAN:	Auto de la Audiencia Nacional.
AIA:	Propuesta de Reglamento sobre Inteligencia Artificial (también conocida como Ley de Inteligencia Artificial).
Apdo/s.:	Apartado, apartados.
CE:	Constitución Española.
CEPD:	Comité Europeo de Protección de Datos.
CHS:	Control Humano Significativo.
COT:	Crimen Organizado Transnacional.
CP:	Código Penal.
DDoS:	Denegación de servicios distribuido.
ECLI:	Identificador Europeo de Jurisprudencia (*European Case Law Identifier*).
EJN:	Red de Periodismo Ético.
EL PAcCTO:	Europa Latinoamérica Programa de Asistencia contra el Crimen Transnacional Organizado.
FGE:	Fiscalía General del Estado.
IA:	Inteligencia Artificial.
IAJ:	Inteligencia Artificial Judicial.
IAP:	Inteligencia Artificial Policial.
IE:	Informe Explicativo.
LAWS:	*Lethal Autonomous Weapons Systems.*
LOPDGDD:	Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales.
LOPJ:	Ley Orgánica del Poder Judicial.
LSE:	Ley de Secretos Empresariales.
MHC:	*Meaningful Human Control* (v. CHS).
ML:	*Machine Learning.*
UN:	Naciones Unidas.
OCDE:	Organización para la Cooperación y el Desarrollo Económicos.

OTAN: Organización del Tratado del Atlántico Norte.
PE: Parlamento Europeo.
RAE: Real Academia Española.
RD-L: Real Decreto-Ley.
RECPC: Revista Electrónica de Ciencia Penal y Criminología.
RGPD: Reglamento General de Protección de Datos.
SAP: Sentencia de Audiencia Provincial.
SEPD: Supervisor Europeo de Protección de Datos.
STS: Sentencia del Tribunal Supremo (Sala Segunda, salvo otra indicación).
STOA: *Panel for the Future of Science and Technology* (Parlamento Europeo).
TC: Tribunal Constitucional.
TEDH: Tribunal Europeo de Derechos Humanos.
TFUE: Tratado de Funcionamiento de la Unión Europea.
TI, TIC: Tecnologías de la Información y la Comunicación.
TJUE: Tribunal de Justicia de la Unión Europea.
TPI: Tribunal Penal Internacional.
TS: Tribunal Supremo.
UE: Unión Europea.
UIT: Unión Internacional de Telecomunicaciones.
UNIDIR: *United Nations Institute for Disarmament Research.*
VioGén: Sistema de Seguimiento Integral de casos de violencia de género.

PRESENTACIÓN

El punto de partida de la presente monografía ha sido la conciencia generalizada de la importancia que han adquirido las tecnologías de la información y de la comunicación (TIC) en el funcionamiento del sistema social en la actualidad, con la utilización de redes y sistemas de tratamiento y comunicación de la información, como medio de crecimiento económico y desarrollo social, tal y como han puesto de manifiesto en diversas investigaciones Romeo Casabona[1] y Rueda Martín[2] y otros participantes en esta obra. Las TIC se han extendido y se han enraizado en nuestras modernas sociedades de modo que han conformado unas estructuras y unas relaciones comerciales, administrativas, laborales, formativas, etc., que trascienden el ámbito estrictamente económico y que son radicalmente nuevas.

La generalización de las TIC y la aparición de la robótica y de los sistemas de inteligencia artificial (IA) ha permitido la identificación o ampliación de nuevos

[1] V. C. M. Romeo Casabona, «Criminal Responsibility of Robots and Autonomus Artificial Intelligent Systems?», Comunicaciones en Propiedad Industrial y Derecho de la Competencia, n.º 91, 2020, pp. 167-187; el mismo, «Riesgo, procedimientos actuariales basados en inteligencia artificial y medidas de seguridad», La justicia en la era de la globalización, P Nicolás Jiménez / L Hernández (dirs.), CGPJ y UPV/EHU, 2018; el mismo, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales, Comares, 2006; el mismo, «Derecho penal y libertades de expresión y comunicación en Internet», La adaptación del Derecho penal al desarrollo social y tecnológico, Romeo Casabona /Sánchez Lázaro (Eds.), Comares, 2010; el mismo, «Arts. 197, 198 y 201», Comentarios al Código penal, Parte Especial II. Títulos VII-XII y faltas correspondientes, Díez / Romeo Casabona (Coords.), Tirant lo blanch, Valencia, 2004; y ya en los inicios del interés por los aspectos penales de estas tecnologías, Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información, Fundesco (Premio de Ensayo de Telefónica), Madrid 1988.

[2] V. M. A. Rueda Martín, «Los ataques contra los sistemas informáticos: conductas de hacking. Cuestiones político-criminales», *La adaptación del Derecho penal al desarrollo social y tecnológico*, Romeo /Sánchez (Eds.), Comares, 2010; la misma, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, Atelier, 2018.

escenarios como, por ejemplo, el comercio electrónico, el acercamiento de los bancos a los clientes —a cambio de un improcedente distanciamiento físico infranqueable—, la administración electrónica entre los poderes públicos y los ciudadanos, la gestión electrónica de los recursos de las empresas o la gestión doméstica. En estos ámbitos enmarcados en la utilización de las TIC se involucran bienes jurídicos tales como el patrimonio, la intimidad personal y familiar, los datos personales, la capacidad competitiva de la empresa u otros bienes jurídicos que afectan a la seguridad nacional de un Estado, de manera que los sistemas de información y comunicación permiten su desarrollo en las modernas sociedades. Como nuestra organización social (la administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, la actividad de las empresas o de los particulares, la enseñanza y la investigación, etc.) ha pasado a depender de forma extraordinaria de unos sistemas y redes de información, los riesgos que se derivan de su vulnerabilidad han exigido garantizar una «Ciberseguridad» en el ciberespacio, es decir, en los sistemas de redes telemáticas, abiertas o cerradas[3].

Este objetivo se ha plasmado expresamente, por ejemplo, en el art. 10 de la Ley 36/2015, de Seguridad Nacional, donde se establece que «se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente». Pero no debemos olvidar tampoco que en la doctrina se ha abierto un nuevo campo de reflexión en los últimos años, focalizado a si los sistemas inteligentes en cuanto tales, en particular aquellos que se vienen denominando sistemas autónomos, serían susceptibles de atribución de responsabilidad penal propia, o bien lo serían los seres humanos responsables de su diseño, funcionamiento, distribución y/o utilización[4]. Estos sistemas llamados autónomos en principio serían capaces de autoaprendizaje y autorreprogramación más allá de su diseño (mediante técnicas *deep learning* y *machine learning*). Vemos cómo se abre un nuevo espacio criminal en el que la ciberseguridad también puede verse involucrada.

El concepto de ciberseguridad, sobre el que, por cierto, no existe unanimidad sobre cómo deba ser entendido, y las necesidades que comporta, se asocia de manera indisoluble y acertadamente, con estructuras tecnológicas, software específico, incluso con sistemas de IA, como primer paso para asegurar aquélla, antes de recurrir a los

[3] Véase en profundidad Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, pp. 47 y ss.

[4] V. Romeo Casabona, «Criminal Responsibility of Robots and Autonomus Artificial Intelligent Systems?», pp. 167 y ss.

instrumentos jurídicos oportunos, sean penales o extrapenales[5]. El reconocimiento de la necesidad de una «Ciberseguridad» se puede explicar por la confluencia de unos intereses que tienen unas notas comunes. Por una parte, los particulares tienen interés en que se proteja la integridad o la confidencialidad de los sistemas informáticos al margen de los contenidos de naturaleza personal o patrimonial que se almacenen en los mismos, como un instrumento que facilita sus relaciones sociales, económicas, con las Administraciones públicas, con el sistema sanitario, etc.[6]. Por otra parte, Los organismos públicos vienen expresando su preocupación creciente por la protección de los sistemas informáticos que almacenan los datos personales de todo tipo o que regulan las relaciones de las distintas administraciones con los administrados, fundamental para el debido funcionamiento de las mismas[7].

Asimismo, las empresas industriales, financieras y de servicios tienen en los modernos sistemas informáticos un instrumento que facilita y potencia su actividad económica y que supone una notable ventaja competitiva en el mercado, y tienen interés en que se proteja no sólo el contenido de la información que almacenan (que puede incluir secretos de empresa, como planes de acción en el mercado, introducción de nuevos productos o instrumentos que respalden su competitividad), sino además la confidencialidad y la integridad de dicho sistema[8]. Para evitar ser víctimas de estos delitos y sufrir pérdidas tanto económicas como de reputación, se hace imperativo conocer los riesgos a los que están expuestas las empresas industriales y poner en marcha mecanismos que eliminen o reduzcan el impacto de la actividad delictiva.

La ciberseguridad se convierte, en consecuencia, en una prioridad, debiendo desarrollarse y actualizarse los procesos orientados a garantizar la seguridad de las empresas e infraestructuras industriales. A nivel interno, en el sector se recomienda el desarrollo de los llamados «planes directores de ciberseguridad», en los que se definen y priorizan los proyectos de seguridad necesarios para cada empresa. A través de los mismos se crean las normativas de uso interno y, posteriormente, los procedimientos de verificación de su cumplimiento.

Por desgracia, en España solo encontramos esta clase de iniciativas en grandes empresas industriales o en aquellas con un alto perfil de exposición a los ataques cibernéticos. Parece necesaria entonces una regulación externa.

[5] Véase *El Código de Derecho de la Ciberseguridad*, BOE, Madrid, 2022 en el enlace https://www.boe.es/biblioteca_juridica/codigos/codigo.php?modo=2&id=173_Codigo_de_Derecho_de_la_Ciberseguridad.

[6] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, p. 61; F Miró Llinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid 2012.

[7] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, p. 61.

[8] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, p. 61.

En el Informe especial 05/2022 sobre Ciberseguridad de las instituciones, órganos y organismos de la UE del Tribunal de Cuentas Europeo, con carácter general, se pone de relieve que el nivel de preparación no es proporcional a las amenazas. Está claro que hace falta también que el Estado vele por el correcto funcionamiento de sus estructuras, de las empresas e infraestructuras industriales y cuente con mecanismos jurídicos para prevenir, perseguir y castigar la actividad criminal. Una herramienta idónea es el CP, toda vez que cuenta con tipos delictivos en los que podrían encuadrarse las vulneraciones de ciberseguridad sufridas. Estas son algunas preguntas que nos planteamos: ¿Requiere el incesante desarrollo tecnológico nuevos tipos delictivos, so riesgo de que las conductas realizadas valiéndose de la última tecnología no encajen en los ya existentes, o basta con una actualización de estos últimos? ¿Merecen siempre los ciberataques el reproche del Derecho Penal, o parte de los mismos podrían ser consideradas de mero interés civil o administrativo? En todo caso, es indudable la necesidad de una investigación profunda y rigurosa en este ámbito que analice los desafíos jurídicos existentes con objeto de garantizar la ciberseguridad de instituciones, órganos y organismos estatales, así como de empresas e infraestructuras industriales.

Además de este interés generalizado debemos observar que la realización de diversas operaciones económicas, financieras, empresariales, laborales, administrativas, etc. por parte de los usuarios tiene que llevarse a cabo de una forma práctica, pero al mismo tiempo segura, es decir, garantizando tanto la disponibilidad del sistema informático como la identidad o la autenticación de la persona que accede a dicho sistema. Los usuarios (particulares, empresas, los poderes públicos, etc.) tienen interés en que cumpliendo unos determinados requisitos se pueda acceder a dichos sistemas informáticos para llevar a cabo aquellas operaciones que sean relevantes, sin que se interpongan demasiados obstáculos[9]. La realidad demuestra que en torno a las TIC y el ciberespacio se ciernen riesgos y amenazas cuya repercusión en la sociedad puede tener elevados costes, entre otras razones por su acusada transversalidad, por lo que recientemente se ha contemplado la intervención del Derecho penal para castigar determinados ataques que suponen una incidencia grave sobre la ciberseguridad. Los costes de los «ciberataques» son evidentes y muy elevados ya que pueden poner en graves dificultades los servicios prestados por las Administraciones públicas, las infraestructuras críticas del Estado o las actividades de las empresas y ciudadanos. Pero también debemos tener presente que los propios Estados pueden ser sujetos activos de estos «ciberataques» a través de sus servicios de inteligencia por sus

[9] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, p. 61.

capacidades militares y de inteligencia que pueden poner en riesgo la Seguridad Nacional y la estabilidad política de nuestro país[10].

En el ámbito internacional y europeo la preocupación por plantear medidas que garanticen una «Ciberseguridad» es manifiesta. El Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001 y la Directiva 2013/40/UE del Parlamento Europeo y del Consejo de la Unión Europea, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, que derogó la Decisión Marco 2005/222/JAI, plantean como propuesta político criminal la protección penal de los sistemas de información mediante, por un lado, la tipificación como delito de conductas de simple acceso no autorizado, intencionado, al conjunto o a una parte del sistema de información. Por otro lado, se contempla la protección penal de los datos informáticos que albergan los sistemas informáticos con el castigo de diversas conductas, que suponen un atentado o una intromisión lesiva (que implica su modificación, inutilización, destrucción, etc.) en la información contenida en dichos sistemas, incluyendo la obstaculización o interrupción de su funcionamiento, por lo que se evidencia adicionalmente una segunda forma de protección penal de los sistemas de información. También se añade la introducción de un amplio número de actos preparatorios que consisten en la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición, sin autorización, de instrumentos como un programa informático o una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información, con la intención de que sean utilizados con el fin de cometer un ataque contra un sistema de información y comunicación, al menos en los casos que no sean de menor gravedad.

El Reglamento General sobre Protección de Datos Personales de 27 de abril de 2016 (UE), aunque sea de forma muy sectorial, ha incorporado a esta nueva normativa europea diversas respuestas no penales sobre la protección y la seguridad de los datos, incluyendo previsiones sobre la circulación transfronteriza de los datos, el derecho de supresión (derecho al olvido) y figuras como el Delegado de Protección de Datos. Teniendo también en cuenta la reciente aprobación en nuestro país del RD-L 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos, es preciso comprobar si hay previsiones en aquél y en este que puedan ser reconducidas de algún modo a la ciberseguridad.

Nuestro CP se ha sumado a esta tendencia político criminal, aunque centrándose en los delitos de descubrimiento y revelación de secretos con la incorporación de figuras delictivas que penalizan determinados ataques contra los sistemas de

[10] V. Maurer, *Cybermercenaries. The State, Hackers and Power*, Cambridge University Press, Cambridge, 2018.

información (p. ej., alterando los datos de un fichero o soporte informático sin estar autorizado, art. 197.2) y la interceptación de datos electrónicos cuando no se trata de una comunicación personal. Destacamos en esta presentación las conductas recogidas en el art. 197 bis del CP que consisten, por una parte, en el acceso o facilitar a otro el acceso, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado al conjunto o una parte de un sistema de información o el mantenimiento dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Por otra parte, en la interceptación de transmisiones no públicas de datos informáticos desde, hacia o dentro de un sistema de información. También se han castigado determinados actos preparatorios de las aludidas conductas en el art. 197 ter del CP. Pero esta regulación se ha centrado, como se ha indicado antes, en los delitos de descubrimiento y revelación de secretos, que, como veremos más abajo, encorseta estos delitos en el angosto marco de la intimidad.

Nuestro ordenamiento jurídico ofrece ya una respuesta normativa en el CP frente a determinadas amenazas en el «ciberespacio». Por un lado, constituye un delito autónomo, el acceso o el facilitar a otro el acceso, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado al conjunto o una parte de un sistema de información o el mantenimiento dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo. Por otro lado, se penaliza la interceptación de transmisiones automáticas, no públicas, de datos informáticos desde, hacia o dentro de un sistema de información con independencia de la información concreta que contengan. Ambas conductas se encuentran castigadas en el artículo 197 bis del CP, dentro del Título X del CP sobre los «*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*». La vinculación de dichos comportamientos con la protección penal de la intimidad personal y familiar plantea algunos interrogantes: ¿se puede castigar por este tipo delictivo al hacker que accede a un sistema de información que almacena datos reservados de personas jurídicas en virtud de lo dispuesto en el art. 200 del CP, o al hacker que accede al sistema informático de una empresa que almacena secretos de empresa, o al hacker que accede a un sistema informático militar que almacena información relevante de la seguridad interior y exterior del estado, con el simple deseo de cumplir ese reto o con la intención de obtener la información contenida en dichos sistemas? (*Cfr.* art. 598 y ss.)[11].

Si partimos de la ubicación sistemática señalada de estos ataques contra los sistemas de información y comunicación, parece que nuestro legislador los ha vinculado únicamente a la protección penal de la intimidad en el sentido de que los sistemas de información deben poder albergar información relevante para la

[11] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, pp. 187, 188 y 189; Fernández Bermejo, Daniel /Martínez Atienza, Gorgonio, *Ciberseguridad, ciberespacio y ciberdelincuencia*, Thomson Reuters- Aranzadi, Cizur menor, 2018, pássim.

intimidad personal y familiar que abarca la vida privada de una persona en la que confluyen numerosos derechos vinculados a la propia personalidad, aunque sea de manera tangencial y no principal, de modo que en ellos se manifieste la pretensión de valor de este bien jurídico. Si, además, acudimos a otros delitos en los que de un modo u otro se protege el secreto en ámbitos diferentes a la intimidad, una primera lectura minuciosa de los mismos parece apuntar que las TIC y el ciberespacio han quedado ajenos a la *mens legislatoris* desde los retos actuales a los que se enfrenta la ciberseguridad[12].

No obstante, no podemos ignorar que estos ataques contra los sistemas de información y comunicación tienen una estrecha relación con otros delitos, de manera que, para cometerlos, con frecuencia, será absolutamente necesario acceder o facilitar el acceso al conjunto o parte de un sistema de información y comunicación, vulnerando las medidas de seguridad establecidas para impedirlo, sin la debida autorización, o interceptar transmisiones automáticas, no públicas, de datos informáticos. A continuación, se exponen los siguientes:

i) Delitos de descubrimiento, revelación o cesión que atentan contra la confidencialidad de los *datos reservados de las personas jurídicas* (art. 200 CP).

ii) *Delito de estafa* (art. 248.2 a) CP, donde se considera reo de estafa a «los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro».

iii) *Delito de utilización de cualquier equipo terminal de telecomunicación* (art. 256 CP), donde se castiga al «que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico», «con la pena de multa de tres a doce meses».

iv) *Delitos de daños informáticos* (arts. 264 y 264 bis CP). En ellos resalta la necesaria vinculación entre la protección de la ciberseguridad y la intervención del Derecho penal, por la gravedad de determinados atentados contra los sistemas de información y comunicación.

En el art. 264 se tipifica la conducta consistente en borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos por cualquier medio, sin autorización y de manera

[12] Una visión mucho más metódica y razonada sobre el hacking la excelente monografía de PILNIK, Franco, *Delitos en el ciberespacio*, Universidad Blas Pascal, Córdoba, 2017, pp. 53 y ss., en donde ofrece la perspectiva cultural, muy diferente a la actual, de lo que se conoció como *hacktivismo*, que surgió en un club de estudiantes del MIT.

grave, cuando el resultado producido fuera grave. Si estos comportamientos han afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la UE o de un Estado Miembro de la UE se contempla una agravación específica. Se considera infraestructura crítica un elemento, sistema o parte de este que sea esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población cuya perturbación o destrucción tendría un impacto significativo al no poder mantener sus funciones.

Asimismo, en el artículo 264 bis se criminaliza al que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo 264; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. Por último, en estas conductas delictivas englobadas dentro del Capítulo IX sobre «los Daños» dentro del Título dedicado a los delitos patrimoniales y contra el orden socio económico se destaca una modalidad comisiva consistente en la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero, introducida en la reforma del Código penal operada por la LO 1/2015.

v) Delitos relativos a la propiedad intelectual (arts. 270 y ss. CP).

vi) Delitos de descubrimiento de secretos de empresa (art. 278 CP), y

vii) Delitos de descubrimiento y revelación de secretos e informaciones relativas a la defensa nacional (art. 598 CP).

En relación con la comisión de este conjunto de infracciones penales acabadas de enumerar, también podemos encontrar la necesidad de acceder o facilitar el acceso al conjunto o parte de un sistema de información y comunicación, vulnerando las medidas de seguridad establecidas para impedirlo, sin la debida autorización, como paso previo para su comisión. En relación con estos delitos se vuelve a poner de manifiesto la necesaria vinculación entre la protección de la ciberseguridad y la intervención del Derecho penal.

Como respuesta a la pregunta planteada, ¿se puede castigar por estos tipos delictivos al hacker que accede a un sistema de información que almacena datos reservados de personas jurídicas, o al hacker que accede al sistema informático de una empresa que almacena secretos de empresa, o al hacker que accede a un sistema informático militar que almacena información relevante de la seguridad interior y exterior del estado, con el simple deseo de cumplir ese reto o con la intención

de obtener la información contenida en dichos sistemas?, tiene que ser negativa si se realiza una interpretación teleológico sistemática del art. 197 bis CP en el sentido explicado anteriormente, ello no resulta satisfactorio[13]. Un sector doctrinal ha propuesto realizar una interpretación teleológica del delito contemplado en el artículo 197 bis, más orientada a la voluntad del legislador europeo y respetuosa con el principio de proporcionalidad, de modo que solamente se deberían entender penalmente relevantes «aquellas conductas de acceso a sistemas de información o de interceptación de datos informáticos pertenecientes a infraestructuras críticas: centrales nucleares, redes de transporte (ferroviario, aéreo o naval) sistema financiero (grandes cantidades de crédito, bolsas, etc., de modo que el concreto acceso o interceptación permita manipular o alterar su funcionamiento»[14].

El fundamento de esta interpretación reside en lo dispuesto en la Directiva 2013/40/UE en cuyo Considerado 3.º se indica que «los ataques contra los sistemas de información y, en particular, los ataques vinculados a la delincuencia organizada, son una amenaza creciente en la Unión y en el resto del mundo, y cada vez preocupa más la posibilidad de ataques terroristas o de naturaleza política contra los sistemas de información que forman parte de las infraestructuras críticas de los Estados miembros y de la Unión. Esta situación pone en peligro la realización de una sociedad de la información segura y de un espacio de libertad, seguridad y justicia y exige, por tanto, una respuesta por parte de la Unión, así como una cooperación y coordinación reforzadas a escala internacional». Y en su Considerando 4.º se define la *infraestructura crítica* como «un elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico y social de la población, como las centrales eléctricas, las redes de transporte y las redes de los órganos de gobierno, y cuya perturbación o destrucción tendría un impacto significativo en un Estado miembro al no poder mantener esas funciones». Sin embargo, como nuestro legislador ha ubicado la protección penal de los sistemas de información en el marco de los delitos contra la intimidad y la propia imagen, esta tesis propuesta por este sector doctrinal atenta contra los principios que se derivan de una interpretación teleológico sistemática[15], al principio de legalidad, en suma,

[13] Véase Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, pp. 187, 188 y 189. Una posición diferente, aun reconociendo su limitado alcance para las personas jurídicas, Romeo Casabona, Carlos M., *Los delitos de descubrimiento y revelación de secretos*, Tirant lo Blanch, Valencia, 2004, pp. 210 y s.; el mismo, «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio», en CM Romeo Casabona, E Sola Reche, MA Boldova Pasamar (Coords.), *Derecho Penal, Parte Especial*, 2.ª ed., Comares, Granada, 2022, p. 293.

[14] Véanse Castiñeira Palou/Estrada i Cuadras, *Lecciones de Derecho penal, Parte Especial,* 7.ª ed. adaptada a la LO 8/2021, Silva Sánchez (Dir.), Ragués i Vallès (Coord.), Atelier, Barcelona, 2021, p. 169.

[15] V. Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, pp. 186 y 187.

pues se propone en último extremo una aplicación analógica de este delito,cuando lo que habría que hacer es cambiar su ubicación en el CP[16]. Aquí se plantea un problema que debe resolverse: ¿cómo debe intervenir nuestro legislador para proteger la ciberseguridad?

Otros aspectos tienen que ver con la incidencia del crimen organizado en diversos ataques contra los sistemas de información y comunicación, de organizaciones terroristas o de las intervenciones de Estados extranjeros[17]. El desarrollo de las TIC ha ampliado el acceso a recursos disponibles para el crimen organizado y para los grupos terroristas, incrementando en relación con estos últimos su capacidad de financiación, reclutamiento, adiestramiento y propaganda. El ciberespacio ofrece unos condicionantes de los que se aprovechan el crimen organizado, las organizaciones terroristas o determinados estados extranjeros, como el carácter anónimo que garantiza el ciberespacio y que facilita conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución. El robo de datos e información, los ataques *ransomware* y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales y los ciberataques contra las infraestructuras críticas son ejemplos de ciberamenazas[18]. El estudio de estrategias normativas para hacer frente de una manera eficaz a estas amenazas constituye uno de los principales retos para la Seguridad. Dentro de estas estrategias es necesario investigar en torno a los actos ilícitos cometidos por el crimen organizado, por organizaciones terroristas a través de internet o servicios conexos y la viabilidad de su penalización[19].

Una de las principales dificultades a las que se enfrenta la persecución eficiente de los delitos relacionados con la ciberseguridad, aparte de la de su calificación jurídico-penal y las carencias que de ello puedan derivarse, es la cuestión de la disposición de un arsenal normativo adaptado a la fenomenología criminológica de los llamados ciberdelitos, con el fin de evitar que estos delitos queden impunes. Y la característica principal es la de su práctica transfronteriza, de modo que puede resultar complejo determinar la ley penal aplicable al caso o, lo que es lo mismo, la

[16] V. C. M. Romeo Casabona, «Delitos contra la intimidad, el Derecho a la propia imagen y la inviolabilidad del domicilio», Romeo/Sola/Boldova (Coords.), *Derecho Penal, Parte Especial,* 2.ª ed., pp. 283 y s.

[17] Sobre las TIC como herramientas de la acción terrorista —muy diversificada— v. Colombani, Jacques-Louis, *Cyberespace et terrorisme*, Les Presses de l'Université Laval, Québec, 2016, pp. 61 y ss.

[18] V. más ampliamente en variadas vertientes y con diversos enfoques jurídico-penales, Brodowski, Dominik, *Cibercrimen y protección de la seguridad informática*, Ad Hoc, Buenos Aires, 2021, pp. 19 y ss.; Wittes & Blum, *The future of violence. Robots and germs, hackers and drones*, Amberley, 2017.

[19] V. Consejo de Europa, *Libro blanco sobre el crimen organizado transnacional*, [trad. al español de A. Perin y C. M. Romeo], Strasbourg, 2016.

jurisdicción competente[20]. Es evidente que la vigencia de la ley penal en relación con estos delitos desde la perspectiva de la soberanía estatal (principio de territorialidad) es totalmente insuficiente. El Convenio Europeo sobre ciberdelincuencia aporta algunas respuestas al respecto, así como instrumentos jurídicos de entreayuda judicial. El Tratado de Prüm de 27 de mayo de 2005, por su parte, incentiva la cooperación judicial y policial (Europol) en relación con la delincuencia transfronteriza, por medio de diversas medidas, que incluyen el intercambio policial de datos. Esto último ha generado importantes dificultades de cooperación, por lo que sigue en pie si tanto el Convenio Europeo sobre ciberdelincuencia como el Tratado de Prüm han satisfecho las expectativas respecto a este tipo de delincuencia.

Existen otros temas relacionados de un modo u otro con la ciberseguridad que están siendo objeto de discusión y presentan un gran interés, como es el caso de la llamada ciberdefensa y, en concreto, de los «Sistemas de Armas Autónomas Letales» (*Letal Autonomous War Systems*: LAWS), o los vehículos automatizados con conducción autónoma, sin piloto. El primer supuesto tiene un tratamiento jurídico prioritario en el derecho internacional de la guerra y humanitario (delitos de lesa humanidad, delitos contra las personas y bienes protegidos en caso de conflicto armado); y en relación con el segundo, por el momento se han producido algunos incidentes, incluidos accidentes mortales, poco explicables en un sistema inteligente que no parecía de entrada desmesuradamente complejo). En consecuencia, dadas las características tan particulares que presentan estas materias, hemos optado por las mantenerlas en un segundo plano.

En esta obra se presentan a los lectores los resultados del trabajo desarrollado en el marco del Proyecto de investigación «Ciberseguridad y ciberdelitos», RTI2018-099306-B-100 (MCIU/AEI/FEDER, UE), del Ministerio de Ciencia, Innovación y Universidades y dentro del Programa Estatal de I+D+i orientado a los Retos de la Sociedad, en el que han participado investigadoras e investigadores de la Universidad del País Vasco (UPV/EHU), Universidad de Zaragoza, Universidad de La Laguna, Universidad de Deusto, Universidad de Brescia (Italia) y del Barcelona Supercomputing Center-Centro Nacional de Supercomputación.

En Leioa y Zaragoza, enero de 2023

Carlos María Romeo Casabona
M.ª Ángeles Rueda Martín
Investigador Principal 1.º Investigadora Principal 2.

[20] Véase Salt, *Nuevos desafíos de la evidencia digital: Acceso transfronterizo y técnicas de acceso remoto a datos informáticos*, Ad-Hoc, Buenos Aires, 2017.

GOBIERNO
DE ESPAÑA

MINISTERIO
DE CIENCIA
E INNOVACIÓN

COMARES
editorial

ISBN 978-84-1369-670-6