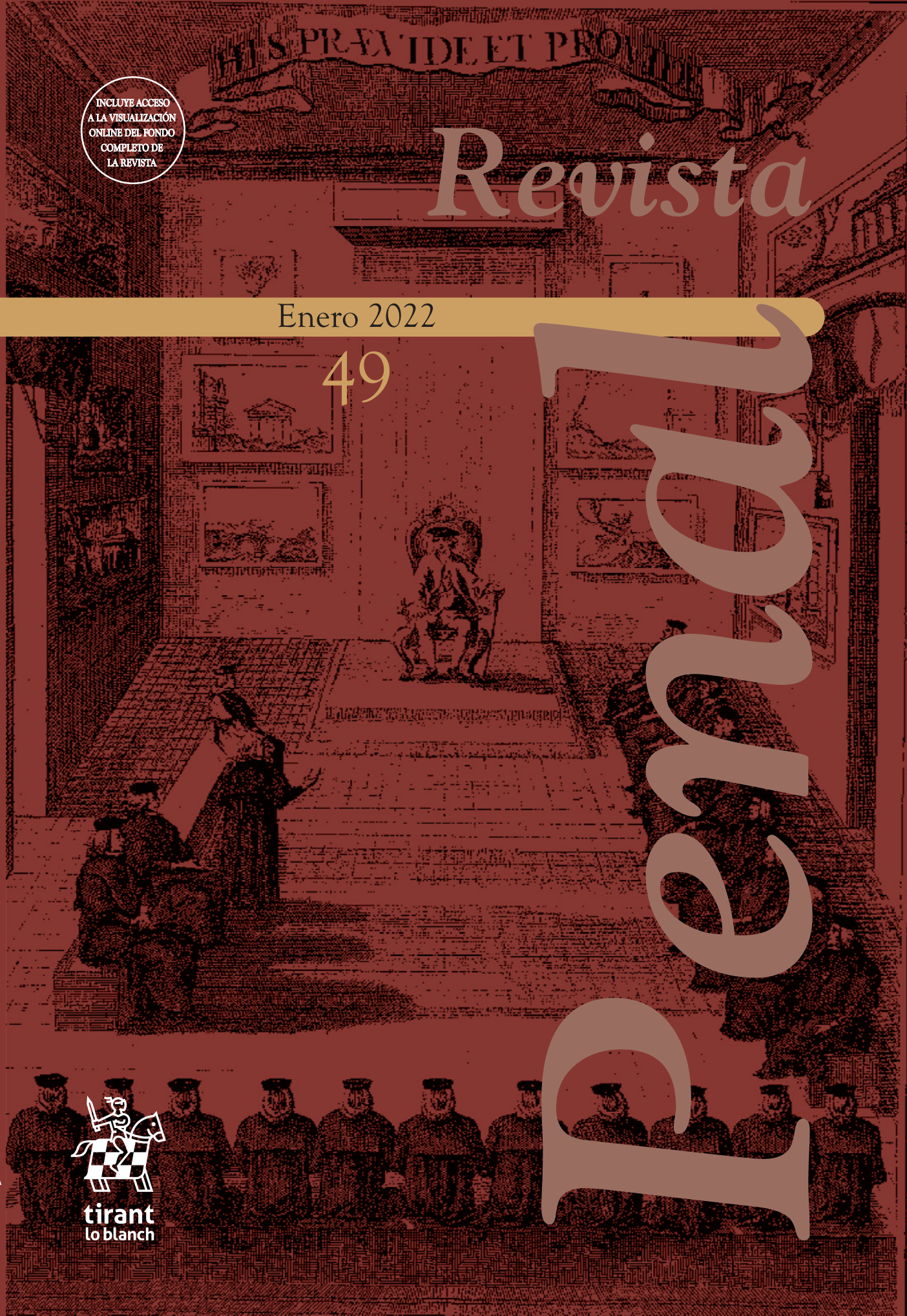
49

INCLUYE ACCESO A LA VISUALIZACIÓN ONLINE DEL FONDO COMPLETO DE LA REVISTA

Revista Penal

Enero 2022

49



Revista Penal

Enero 2022

tirant lo blanch

tirant lo blanch

Revista Penal

Número 49

Sumario

* *Los primeros 25 números de la Revista Penal están recogidos en el repositorio institucional científico de la Universidad de Huelva Arias Montano:* http://rabida.uhu.es/dspace/handle/10272/11778

tirant lo blanch

Publicación semestral editada en colaboración con las Universidades de Huelva, Salamanca, Castilla-La Mancha, y Pablo Olavide de Sevilla

Dirección

Juan Carlos Ferré Olivé. Universidad de Huelva
jcferreolive@gmail.com

Secretarios de redacción

Víctor Manuel Macías Caro. Universidad Pablo de Olavide
Miguel Bustos Rubio. Universidad Internacional de La Rioja

Comité Científico Internacional

Kai Ambos. Univ. Göttingen
Luis Arroyo Zapatero. Univ. Castilla-La Mancha
Ignacio Berdugo Gómez de la Torre. Univ. Salamanca
Gerhard Dannecker. Univ. Heidelberg
José Luis de la Cuesta Arzamendi. Univ. País Vasco
Norberto de la Mata Barranco, Univ. País Vasco
Albin Eser. Max Planck Institut, Freiburg
Jorge Figueiredo Dias. Univ. Coimbra
George P. Fletcher. Univ.Columbia
Luigi Foffani. Univ. Módena
Nicolás García Rivas. Univ. Castilla-La Mancha
Juan Luis Gómez Colomer. Univ. Jaume Iº
Carmen Gómez Rivero. Univ. Sevilla
José Luis González Cussac. Univ. Valencia
Victor Moreno Catena. Univ. Carlos III
Carlos Martínez- Buján Pérez, Univ. A Coruña
Alessandro Melchionda. Univ. Trento
Francisco Muñoz Conde. Univ. Pablo Olavide
Francesco Palazzo. Univ. Firenze
Teresa Pizarro Beleza. Univ. Lisboa
Claus Roxin. Univ. München
José Ramón Serrano Piedecasas. Univ. Castilla-La Mancha
Ulrich Sieber. Max Planck. Institut, Freiburg
Juan M. Terradillos Basoco. Univ. Cádiz
John Vervaele. Univ. Utrecht
Eugenio Raúl Zaffaroni. Univ. Buenos Aires
Manuel Vidaurri Aréchiga. Univ. La Salle Bajío

Consejo de Redacción

Miguel Ángel Núñez Paz y Susana Barón Quintero (Universidad de Huelva), Adán Nieto Martín, Eduardo Demetrio Crespo y Ana Cristina Rodríguez (Universidad de Castilla-La Mancha), Emilio Cortés Bechiarelli (Universidad de Extremadura), Fernando Navarro Cardoso y Carmen Salinero Alonso (Universidad de Las Palmas de Gran Canaria), Lorenzo Bujosa Badell, Eduardo Fabián Caparros, Nuria Matellanes Rodríguez, Ana Pérez Cepeda, Nieves Sanz Mulas y Nicolás Rodríguez García (Universidad de Salamanca), Paula Andrea Ramírez Barbosa (Universidad Externado, Colombia), Paula Bianchi (Universidad de Los Andes, Venezuela), Elena Núñez Castaño (Universidad de Sevilla), Carmen González Vaz (Universidad Isabel Iº, Burgos), José León Alapont (Universidad de Valencia), Pablo Galain Palermo (Universidad Nacional Andrés Bello de Chile), Alexis Couto de Brito y William Terra de Oliveira (Univ. Mackenzie, San Pablo, Brasil).

Sistemas penales comparados

Eva Rulands (Alemania)
Luis Fernando Niño (Argentina)
Alexis Couto de Brito y Jenifer Moraes (Brasil)
Paula Andrea Ramírez Barbosa (Colombia)
Angie A. Arce Acuña (Costa Rica)
Elena Núñez Castaño (España)
Lavinia Messori (Italia)
Manuel Vidaurri Aréchiga (México)
Sergio J. Cuarezma Terán (Nicaragua)
Campo Elías Muñoz Arango (Panamá)
Víctor Roberto Prado Saldarriaga (Perú)
Blanka Julita Stefańska (Polonia)
Frederico de Lacerda Costa Pinto (Portugal)
Volodymyr Hulkevych (Ucrania)
Pablo Galain Palermo y Renata Scaglione (Uruguay)
Jesús Enrique Rincón Rincón (Venezuela)

www.revistapenal.com

© TIRANT LO BLANCH
EDITA: TIRANT LO BLANCH
C/ Artes Gráficas, 14 - 46010 - Valencia
TELFS.: 96/361 00 48 - 50
FAX: 96/369 41 51
Email:tlb@tirant.com
http://www.tirant.com
Librería virtual: http://www.tirant.es
DEPÓSITO LEGAL: B-28940-1997
ISSN.: 1138-9168
MAQUETA: Tink Factoría de Color

Si tiene alguna queja o sugerencia envíenos un mail a: *atencioncliente@tirant.com*. En caso de no ser atendida su sugerencia por favor lea en *www.tirant.net/index.php/empresa/politicas-de-empresa* nuestro procedimiento de quejas.

Responsabilidad Social Corporativa: http://www.tirant.net/Docs/RSCTirant.pdf

Los ataques de denegación de servicios como ciberdelito en el Código Penal español

Mª Ángeles Rueda Martín

Revista Penal, n.º 49 - Enero 2022

Ficha Técnica

Autor: Mª Ángeles Rueda Martín
Adscripción institucional: Catedrática de Derecho Penal, Universidad de Zaragoza
Title: Attacks of denial of services as cybercrime in the spanish penal code

Summary: INTRODUCTION. II. THE ATTACKS OF DENIAL OF SERVICES OF THE INFORMATION AND COMMUNICATION SYSTEMS IN THE INTERNATIONAL FIELD AND OF THE EUROPEAN UNION: CRIMINAL POLITICAL PROPOSAL. III. THE LEGAL PROPERTY PROTECTED IN THE CRIME OF DENIAL OF SERVICES OF THE INFORMATION AND COMMUNICATION SYSTEMS. REFLECTIONS ON YOUR CRIMINAL PROTECTION. IV. POLITICAL CRIMINAL OPTIONS TO TYPE THE ATTACKS OF DENIAL OF SERVICES OF THE INFORMATION AND COMMUNICATION SYSTEMS. V. THE BASIC TYPE OF THE CRIME OF DENIAL OF SERVICES OF THE INFORMATION AND COMMUNICATION SYSTEMS. V. SPECIFIC AGGRAVATIONS. 1) The obstruction or interruption of the operation of a foreign computer system in a serious way within the framework of a criminal organization. 2) Damages of particular gravity, damage to a large number of computer systems or serious damage to the operation of essential public services or the provision of basic necessities. 3) Affecting the information

183

system of a critical infrastructure or creating a serious danger to the security of the State, the European Union or a Member State of the European Union. 4) Commission of the fact by the use of certain instruments. 5) Facts of extreme gravity. 6) The obstruction or interruption of the operation of a third-party computer system in a serious way through the illicit use of personal data of another person to facilitate access to the computer system or to gain the trust of a third party. SAW. PUNISHABLE PREPARATORY ACTS. VII. CRIMINAL LIABILITY OF LEGAL PERSONS. VIII. REFLECTIONS AROUND THE DETERMINATION OF THE CRIMINAL LAW APPLICABLE IN ATTACKS OF DENIAL OF CROSS-BORDER SERVICES. IX. DOES THE PENALTY OF ATTACKS OF DENIAL OF SERVICES AS A CYBERCRIME IN THE SPANISH CRIMINAL CODE, DOES IT OFFER AN ADEQUATE RESPONSE TO THE THREATS AND ATTACKS THAT ARE CLOSED ON CYBER SECURITY? X. BIBLIOGRAPHY.

Resumen: El objetivo que tiene esta investigación reside en analizar la regulación penal adoptada en nuestro país en torno a los ataques de denegación de servicios de los sistemas de información, con el fin de estudiar su estructura y elementos típicos, valorar su adecuación a los posibles avances tecnológicos del ciberespacio y ofrecer, en su caso, alternativas que permitan su adaptación a los nuevos ataques a las redes de comunicación e información que el ciberespacio une.
Palabras clave: Ciberdelincuencia, ciberdelitos, bien jurídico

Abtract: The objective of this research is to analyze the criminal regulation adopted in our country around the attacks of denial of services of information systems, in order to study their structure and typical elements, assess their adequacy to possible technological advances cyberspace and offer, where appropriate, alternatives that allow its adaptation to new attacks on the communication and information networks that cyberspace unites.
Keywords: Cybercrime, cybercrimes, legally protected good

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

Rec.: 13-08-2021 **Fav**.: 15-09-2021

I. INTRODUCCIÓN

Las manifestaciones delictivas relacionadas con las tecnologías de la información y comunicación (en adelante TIC) son muy variadas y también abundantes. Señalar las notas características comunes de dichas manifestaciones constituye una tarea compleja, porque su aparición va indisolublemente unida a la irrupción de nuevas herramientas y técnicas utilizadas en el tratamiento y la transmisión de la información y de la comunicación en constante evolución. Con dichas herramientas y técnicas se ha creado un espacio virtual, no físico, el ciberespacio, determinado por la interconexión de personas a través de infraestructuras de TIC, y dentro de él, uno de sus principales catalizadores es Internet, sistema global de información y comunicación basado en el protocolo TCP que une ordenadores de todo el mundo y permite el acceso a cualquiera de ellos para obtener e intercambiar información de manera sencilla[1]. En este ámbito el Derecho

1 Véase la definición del ciberespacio ofrecida por Miró LLinares, *El cibercrimen,* p. 144, nota 6; más ampliamente pp. 145 y ss. De manera similar Álvarez Rodríguez, «Constitución y Derecho del Ciberespacio», p. 22; Barrio Andrés, *Manual de Derecho digital*, pp. 50 y 51; Fernández Bermejo/Martínez Atienza, *Ciberseguridad, ciberespacio y ciberdelincuencia*, pp. 113 y 116.

En la Estrategia Nacional de Ciberseguridad de 2019 que establece la posición de España ante una nueva concepción de la ciberseguridad (Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional), se define el ciberespacio como un espacio común global caracterizado por: a) su apertura funcional y su dinamismo; b) la conectividad universal que facilita el libre flujo de información, servicios e ideas, y amplía su dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales; c) su impulso del emprendimiento, el progreso socioeconómico y las nuevas posibilidades que ofrece a todos los sectores en los que se desarrollan actividades ya sean públicas o privadas. Sus implicaciones

penal se encuentra ante el problema de adaptar la aplicación de sus tipos penales a una realidad nueva y muy cambiante, lo que implica un riesgo evidente de falta de adecuación de la legislación penal por la rapidez de los avances tecnológicos. Un ejemplo muy ilustrativo de la necesidad de esta adaptación lo encontramos en los ataques a los sistemas de información y comunicación que ocasionan bloqueos en los servicios que prestan[2]. En el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información se definen los ataques de denegación de servicios desde un punto de vista técnico, como el conjunto de procedimientos que tienen por objetivo saturar con peticiones de servicio un servidor, hasta que este no puede atenderlas, provocando su colapso e impidiendo que los usuarios legítimos puedan utilizar los servicios que presta[3]. Con carácter general, los comportamientos que producen la interrupción del servicio que proporcionan los sistemas de información y comunicación tienen en común cuatro notas: en primer lugar, para su comisión es preciso que, previamente, se haya realizado un acceso o se haya facilitado a otro el acceso al conjunto o a una parte de un sistema de información, ya sea de manera lícita o ilícita en la mayor parte de los casos, o se haya producido un mantenimiento en el mismo en contra de la voluntad de la voluntad de quien tenga el legítimo derecho a excluirlo. En segundo lugar, estos comportamientos recaen sobre los sistemas informáticos para impedir su funcionamiento, destruirlos o modificarlos, ocasionando una denegación de los servicios que dispensan con consecuencias perjudiciales[4]. Normalmente, el *modus operandi* consiste en la sobrecarga de un servidor con múltiples solicitudes que bloquean el funcionamiento óptimo del correspondiente sitio web[5], y puede unirse a cualquier otra manifestación de sabotaje cibernético en sentido amplio. En tercer lugar, los ataques de denegación de servicios de los sistemas de información constituyen un ciberdelito que únicamente es posible cometer en el ciberespacio[6]. En cuarto lugar, los ciberataques que afectan al funcionamiento de los sistemas de información y comunicación conllevan una vulneración de las medidas de seguridad establecidas para impedirlos.

En nuestro Código penal se penalizan los ataques de denegación de servicios de los sistemas de información y comunicación desde la reforma operada por la LO 5/2010, de 22 de junio, que contempló por primera vez en el art. 264.2 en el Capítulo IX, *De los daños*, del Título XIII, *Delitos contra el patrimonio y contra el orden socioeconómico,* un nuevo delito consistente en obstaculizar o interrumpir el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimien-

---

van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

2 Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 41.

3 Asimismo, se indica que los ataques de denegación distribuida de servicios (DDoS) constituyen una variante en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de bots, generalmente sin el conocimiento de los usuarios.

4 Véase el Informe de Ciberamenazas y Tendencias en su edición de 2019 CCN-CERT IA-13/19, elaborado por la Capacidad de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional (CCN-CERT), pp. 41 y ss.; 89 y ss.

5 Véase Renobell Santaren, «Hacktivismo digital: de la cultura hacker a los delitos digitales», p. 258.

6 Sobre los caracteres del ciberespacio y sus implicaciones en la dogmática penal, véase el reciente trabajo de López Gorostidi, «Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: apropósito del confinamiento provocado por la crisis sanitaria del COVID-19», pp. 130 y ss. Stytz/Bank, «Cyber Warfare Simulation to Prepare to Control Cyber Space», *National Cybersecurity Institute Journal*, 2014, vol 1, nº 2, p. 10 definen el ciberespacio con los siguientes elementos: 1) datos; 2) tecnologías informáticas (como hardware informático, software informático, redes/infraestructura informática, protocolos de red, virtualización y computación en la nube); 3) tecnologías de análisis/comprensión de la información (como virtualización de la información, colaboración y tecnologías de datos); y 4) tecnologías de interacción/gestión de la información (como interacción persona-ordenador, tecnologías de agentes inteligentes, inferencia de intenciones humanas, tecnologías de personalización y tecnologías de bases de datos). Un ciberataque es un ataque a cualquiera de estos cuatro elementos.

En concreto, los ataques de denegación de servicios suponen una clara manifestación de ciberataques puros, porque las TIC son su objeto y constituyen el medio por el cual se cometen y porque sus efectos tienen lugar en el ciberespacio, donde existe una conectividad universal que facilita el libre flujo de información, servicios e ideas, y una dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales. Véanse las características generales de los ciberataques puros expuestas por Miró LLinares, *El cibercrimen,* pp. 52 y ss.; Romeo Casabona, «De los delitos informáticos al cibercrimen: una aproximación conceptual y político-criminal», *passim*. En el art. 1.3 del Reglamento (UE) 2019/796 del Consejo de la Unión Europea, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, se definen los ciberataques como aquellas «acciones que implican cualesquiera de los siguientes elementos: a) acceso a sistemas de información; b) intromisión en sistemas de información; c) intromisión en datos; o d) interceptación de datos, cuando dichas acciones no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de los datos, o de parte de los mismos, o no estén permitidas por el Derecho de la Unión o de un Estado miembro».

do o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave. Posteriormente, la LO 1/2015, de 30 de marzo, ha trasladado este delito al art. 264 bis del Código penal, ampliando sus modalidades comisivas: «1. Será castigado con la pena de prisión de seis meses a tres años el que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno: a) realizando alguna de las conductas a que se refiere el artículo anterior[7]; b) introduciendo o transmitiendo datos; o c) destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático, telemático o de almacenamiento de información electrónica. Si los hechos hubieran perjudicado de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado. 2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero». En el art. 264 ter se castigan, además, como actos preparatorios la producción, la adquisición para su uso, la importación o la facilitación a terceros, de cualquier modo, con la intención de cometer alguno de los delitos a que se refieren los arts. 264 y 264 bis, de: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

El objetivo que tiene esta investigación reside en analizar la regulación penal adoptada en nuestro país en torno a los ataques de denegación de servicios de los sistemas de información y comunicación, con el fin de estudiar su estructura y elementos típicos y valorar su adecuación a los posibles avances tecnológicos del ciberespacio. La necesidad de este estudio se justifica también por las circunstancias en las que se ha desarrollado nuestra vida por la pandemia ocasionada por el virus SARS-CoV-2, que nos ha obligado a depender más si cabe del buen funcionamiento de los servicios que proporciona el ciberespacio en prácticamente todos los ámbitos de nuestra vida[8]. Antes de analizar y valorar esta regulación penal conviene abordar, brevemente, los planteamientos político-criminales en torno al delito de denegación de servicios de los sistemas de información en el ámbito internacional para, seguidamente, estudiar la opción por la que se ha decantado nuestro legislador en el art. 264 bis del Código penal español y sus elementos estructurales.

II. LOS ATAQUES DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL ÁMBITO INTERNACIONAL Y DE LA UNIÓN EUROPEA: PROPUESTA POLÍTICO CRIMINAL

La criminalización de los ataques de denegación de servicios de los sistemas de información constituye una propuesta político criminal constante en el ámbito internacional. En el art. 5 del Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de

7 El artículo 264 del Código penal dispone que «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. 2. Se impondrá una pena de prisión de dos a cinco años y multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1.ª Se hubiese cometido en el marco de una organización criminal. 2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. 4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará 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. 5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado. 3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero».

8 Véanse al respecto las advertencias de EUROPOL en su informe de 2020 «Catching the virus cybercrime, disinformation and the COVID-19 pandemic», disponible en el enlace https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

Véase también el trabajo de Miró LLinares, «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos», pp. 4 y ss.

noviembre de 2001)[9], se contempla que «*Cada Parte adoptará las medidas necesarias y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos*»[10]. En el art. 4 de 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, también se prevé que «*Los Estados miembros adoptarán las medidas necesarias para que la obstaculización o la interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad*»[11]. Por otra parte, en el art. 1.3 del Reglamento (UE) 2019/796 del Consejo de la Unión Europea, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, se define como un ciberataque, entre otros, la intromisión en sistemas de información conceptuada como la «obstaculización o interrupción del funcionamiento de un sistema de información introduciendo datos digitales, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo tales datos, o haciéndolos inaccesibles» (art. 1.7).

La propuesta político criminal contenida en los textos normativos indicados es uniforme al plantear la criminalización de ataques contra los sistemas de información que consistan en la obstaculización o en la interrupción de su funcionamiento, siempre que revistan una determinada gravedad. También merece la pena poner de relieve que tanto en el Convenio del Consejo de Europa sobre Cibercriminalidad como en la Directiva 2013/40/UE se exige que la denegación de servicios de un sistema de información se realice, únicamente, a través de la introducción, transmisión, daño, borrado, deterioro, alteración, supresión o —en la Directiva 2013/40/UE— haciendo inaccesibles datos informáticos.

III. EL BIEN JURÍDICO PROTEGIDO EN EL DELITO DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN. REFLEXIONES SOBRE SU PROTECCIÓN PENAL

Vamos a analizar a continuación cuál es el bien jurídico protegido en el delito de denegación de servicios de los sistemas de información contemplado en el art. 264 bis del Código penal para estudiar, posteriormente, su estructura y elementos típicos. Este comportamiento delictivo presenta un indudable parentesco con el tipificado en los arts. 197 bis y 197 ter del Código penal, dentro del Título X, *Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*[12], en los que el objeto de protección directo son

9 Sobre el proceso de gestación de este Convenio, véanse, Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre *Cyber-Crime»,* pp. 16-25; Lezertúa, «El proyecto de Convenio sobre el cybercrimen del Consejo de Europa», pp. 17 y ss. Asimismo, véanse, Morón Lerma/Rodríguez Puerta, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», pp. 167 y ss.; Sánchez Bravo, «El Convenio del Consejo de Europa sobre cibercrimen: control vs. Libertades públicas», pp. 1851 y ss.; Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre *Cyber-Crime»,* pp. 26 y ss.; Rodríguez Bernal, «Los cibercrímenes en el espacio de libertad, seguridad y justicia», pp. 12 y ss.

10 En este convenio se plantea también el castigo de un amplio abanico de actos preparatorios consistentes no solo en la producción, venta, utilización, importación, distribución o cualquier forma de puesta a disposición de: a) cualquier dispositivo concebido o adaptado para cometer cualquiera de los delitos recogidos en los arts. 2 a 5 del Convenio; o b) una contraseña, código de acceso o datos informáticos similares con la finalidad de cometer las infracciones de los mencionados preceptos, sino que alcanza también la mera posesión de algunos de estos elementos con la misma intención.

11 En el art. 7 de la Directiva 2013/40/UE se propone asimismo penalizar la utilización de determinados instrumentos para cometer el conjunto de infracciones entre las que se encuentra la que constituye nuestro objeto de estudio: «Los Estados miembros adoptarán las medidas necesarias para garantizar que la producción intencional, venta, adquisición para el uso, importación, distribución u otra forma de puesta a disposición de los siguientes instrumentos, sin autorización y con la intención de que sean utilizados con el fin de cometer cualquiera de las infracciones mencionadas en los artículos 3 a 6, sea sancionable como infracción penal, al menos en los casos que no sean de menor gravedad: a) un programa informático, concebido o adaptado principalmente para cometer una infracción de las mencionadas en los artículos 3 a 6; 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». Y en determinados apartados del art. 9 se recogen algunas circunstancias agravantes como, entre otras, la afectación a un número significativo de sistemas de información o a un sistema de información de una infraestructura crítica, la causación de daños graves, o la utilización ilícita de datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad.

12 El art. 197 bis dispone que «1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información

también los sistemas de información[13]. En relación con el bien jurídico protegido en el delito consistente en un acceso ilícito a sistemas de información tipificado en el art. 197 bis, Morón Lerma estima que asistimos a «un nuevo valor social, un interés de nuevo cuño, cifrado en la seguridad de los sistemas informáticos, o en la seguridad informática, o en la seguridad en el funcionamiento de dichos sistemas informáticos». A juicio de esta autora «parece emerger un interés difuso, inmaterial, digno de tutela, pero que, en ningún caso, puede ser identificado, apriorísticamente, con un bien jurídico merecedor de protección penal»[14]. Puente Aba se refiere también al interés relativo a la "seguridad informática", aunque se manifiesta en contra de su configuración como bien jurídico protegido porque no es acorde con los principios de intervención mínima del Derecho penal y con el principio de proporcionalidad[15]. No obstante, otro sector doctrinal considera que la seguridad en los sistemas informáticos sí puede ser considerado el bien jurídico protegido en estos comportamientos, merecedor de protección penal, de carácter supraindividual y difuso[16]. Desde mi punto de vista, con carácter general, estas definiciones de bienes jurídicos que hacen referencia a la seguridad en relación con el delito que penaliza el acceso no autorizado a sistemas informáticos se caracterizan, de una manera explícita o implícita, por la descripción de una situación de ausencia de riesgos o de lesión para determinados bienes jurídicos que se pueden involucrar en los sistemas de comunicación e información como el patrimonio, la capacidad competitiva de la empresa, la propiedad intelectual, la intimidad personal y familiar, etc. Ahora bien, el valor de la seguridad como bien jurídico no le dota de autonomía, es decir, le impide atribuir a este substrato un valor homogéneo, unitario y autónomo porque no hay una seguridad en sí misma si no es puesta en relación con estos otros bienes jurídicos[17/18].

Por otra parte, también se ha concluido que el bien jurídico protegido en el delito de acceso ilícito a sistemas de información es la inviolabilidad del domicilio

o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años. 2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses». El art. 197 ter establece que «Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis: a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información».

13 Véase al respecto Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código pena*l, Atelier, Barcelona, 2018, pp. 47 y ss.

14 Véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 85; la misma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», p. 106.

15 Véase Puente Aba, «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», pp. 398 y ss.

16 Véanse Gutiérrez Francés, *Fraude informático y estafa*, pp. 619-620; la misma, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», p. 1183; Mir Puig, «Sobre algunas cuestiones relevantes del derecho penal en internet», p. 303; Miró LLinares, «Delitos informáticos. Hacking. Daños», marginal nº. 1439; Tomás y Valiente Lanuza, *Comentarios prácticos al Código penal, art. 197*, p. 655; Matellanes Rodríguez, «Vías para la tipificación del acceso ilegal a los sistemas informáticos (II)», p. 68; Anarte Borrallo/Doval País, *Derecho penal, Parte Especial,* 2ª ed., p. 512; Romeo Casabona, *Derecho penal, Parte Especial*, p. 270; Colás Turégano, «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)», p. 664. Véase en este sentido la Circular 3/2017 de la Fiscalía General del Estado, p. 3.

17 Como apunta González Rus «tal como aparece concebida y formulada, la seguridad informática no tiene aún, a mi juicio, un contenido sustancial lo suficientemente elaborado y preciso como para permitir una construcción certera de la tutela penal. Prueba de ello es que unas veces se la relaciona con el honor, el patrimonio y la intimidad, y otras, además, con la libertad de información, el secreto de las comunicaciones, la libertad de expresión, etcétera, lo que dice bastante de la ambigüedad del concepto»; véase González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», p. 21. En este sentido advierten también Anarte Borrallo/Doval País, *Derecho penal, Parte Especial,* 2ª ed., p. 517 que la seguridad de los sistemas de información «sitúa al intérprete ante un objeto protegido que carece de un sustrato material propio (como siempre ocurre cuando se apela a la *seguridad* de algún objeto)».

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

informático[19]. Por ejemplo, para Morales García el concepto de domicilio informático se centra en el «derecho a mantener los espacios de actuación en red y su contenido al margen de los accesos no deseados, tal como sucede, *ceteris paribus*, con el domicilio "físico"», de modo que el domicilio informático lo configura «la información vital que se sitúa en esos espacios que, por tal razón, dada la absoluta miscelánea de elementos privados, públicos, confidenciales, íntimos, reservados, compartibles, etc., determina la reserva del espacio en términos de derecho a la intimidad»[20]. En la SAP de Vizcaya Sección 2 nº. 90307/2014, de 23 julio **(**ECLI:ES:APBI:2014:1696**)**, se alude también a este bien jurídico "domicilio informático": «el artículo 197.3 del código penal establece que "el que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años", siendo este delito el denominado de intromisión informática en que lo se protege es la libertad informática o más exactamente el domicilio informático de una persona, no siendo relevante la naturaleza de los datos contenidos en el sistema informático pudiendo ser de naturaleza personal, familiar, económicos o de otra índole que pertenezcan al ámbito privado de dicha persona». Esta definición del bien jurídico protegido tampoco resulta plenamente convincente, porque limita excesivamente el objeto de protección a la existencia de un espacio "informático" que alberga información vital y, por ello, merecedor de intervención penal. Desde luego que existe este interés en la protección de dicho espacio —que puede encontrar un paralelismo con el bien jurídico "inviolabilidad del domicilio"—, pero no es el único interés que se constata cuando se plantea penalizar conductas que suponen determinados ataques a sistemas de información, tal y como se puede deducir de las propuestas político criminales contenidas en el Convenio del Consejo de Europa sobre Cibercriminalidad y en la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información. Por el contrario, hay también un interés en garantizar la confidencialidad e integridad de dichos sistemas por el valor que han adquirido en nuestro desarrollo económico, social y personal, valor que trasciende la necesidad de preservar un simple espacio "informático".

Otro sector doctrinal ha afirmado la existencia de un nuevo bien jurídico protegido, estrictamente informático, que es objeto de lesión o puesta en peligro en todos los delitos que tienen como objeto un sistema de información: la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, de manera que estaremos ante un delito informático, o dicho con mayor precisión un ciberdelito, cuando se realice una conducta que lesione o ponga en peligro dicho bien jurídico[21]. Por ejemplo, Carrasco Andrino afirma que «se trata de preservar la indemnidad (integridad, confidencialidad, disponibilidad) de los sistemas informáticos como contenedores de información sensible para la intimidad, el honor, el patrimonio, etc. y de los que dependen, además, las infraestructuras y los servicios electrónicos en la nueva Sociedad de la Información»[22]. En una dirección similar se ha pronunciado Morales Prats quien considera que «la protección del Derecho penal se orienta a proteger las redes y sistemas de información, por cuanto la seguridad de los mismos y su capacidad de resistencia es lo que garantiza la confianza y la certidumbre en la autenticidad e integridad de la información que se contiene en esos sistemas y esas redes. La apuesta es, por tanto, de acuerdo con Carrasco Andrino, por la seguridad en el tráfico informático y por proteger de manera mediata tras la reforma de 2015, la integridad y certeza en los datos y programas informáticos»[23]. De la Mata Barranco plantea también que el bien jurídico protegido en el delito tipificado en el art. 197 bis del Código penal es la seguridad en el uso de los sistemas de información tutelando su confidencialidad y su integridad, por lo que en sí implica para el desarrollo de las relaciones sociales, de modo que ««habrá que esperar que el legislador español aborde globalmente la cuestión del tratamiento de la

19 Véanse, Alonso de Escamilla, *Delitos,* 3ª ed., p. 223; Morales García, «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248», p. 185.

20 Véase Morales García, «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248», p. 185.

21 Véase al respecto Rueda Martín, *La nueva protección de la vida privada y de los sistemas de información en el Código penal*, pp. 47 y ss.; Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e internet», p. 260, 261, 262 y 269; Sieber, «Legal Aspects of Computer-Related Crime in the Information Society —Comcrime-Study—, prepared for the European Commission by Frof. Dr. Ulrich Sieber, versión de enero de 1998, p. 42, se refiere también a la integridad del sistema informático que resulta vulnerada con las conductas denominadas *hacking*; Almenar Pineda, *El delito de hacking*, p. 139.

22 Véase Carrasco Andrino, *Derecho penal español, Parte Especial (I)*, 2ª ed., p. 783.

23 Véase Morales Prats, *Comentarios al Código Penal Español, Tomo I (artículo 197*), 7ª ed., p. 1478. De forma similar también González Cussac, *Derecho penal, Parte Especial*, 5ª ed., p. 255; Castelló Nicas, «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor», p. 505.

delincuencia contra datos y sistemas informáticos entendiendo lo que implica la lesividad de estos ataques y habrá que esperar que asuma decididamente un planteamiento en que se atienda la idea de seguridad en el uso de los sistemas de información y comunicación»[24].

Si nos centramos en el delito de obstaculización o interrupción del funcionamiento de un sistema de información ajeno de una manera grave, en relación con el bien jurídico protegido se suele poner en un primer plano como objeto de protección el patrimonio al encontrarse en el Capítulo IX, *De los daños*, del Título XIII, *Delitos contra el patrimonio y contra el orden socioeconómico*[25]. No obstante, los ataques a los sistemas de información vulneran o ponen en peligro numerosos intereses que pueden ser individuales o colectivos, plurales y variados. Reducir el bien jurídico protegido en este delito a su dimensión patrimonial, puede conllevar la exclusión de comportamientos que afecten a otros intereses diferentes que deben ser atendidos también, porque configuran unas estructuras y unas relaciones comerciales, administrativas, laborales, formativas, etc., que trascienden el ámbito estrictamente económico y que son radicalmente nuevas[26]. Por ejemplo, Miró LLinares, aunque afirma que «la inutilización de un sistema informático por el motivo que sea, también debe valorarse como una pérdida en sentido económico»[27], reconoce que la ubicación de los ataques de denegación de servicios en los delitos contra el patrimonio «no resulta tan evidente, dada la naturaleza plural de los intereses que se pueden ver afectados por tal comportamiento ilícito en internet. De hecho, su situación como delito patrimonial puede conllevar la no consideración de la dimensión de afectación a la libertad de emisores y receptores en internet de servicios de gran importancia social»[28]. En el delito de Computersabotage del § 303b del StGB, la doctrina alemana estima mayoritariamente que el bien jurídico protegido es la funcionalidad del procesamiento de datos[29]. Sin embar-

24 Véase De la Mata Barranco, «Reflexiones sobre el bien jurídico a proteger en el delito de acceso informático ilícito (art. 197 bis del Código penal). El concepto de privacidad informática y la tutela del buen funcionamiento de los sistemas de información y comunicación», p. 86. No obstante, continúa este autor «en todo caso, mientras no lo haga y siga atendiendo la tutela de intereses tradicionales (tal como refleja la ubicación del art. 197 bis), lo que sí al menos debe aceptarse es que ya ni importa la intimidad, ni importa el secreto ni importa lo personal. Importa la idea de privacidad informática»; véase el mismo, ob. cit., p. 86. En nuestra jurisprudencia en alguna sentencia se habla de la intimidad informática como bien jurídico protegido, como sucede con la SAP de Madrid sec 2 nº. 329/2015, de 27 abril (ECLI:ES:APM:2015:6026), en la que se afirma que: «este nuevo subtipo, sanciona el acceso inconsentido a informaciones ubicadas en el sistema informático (datos, programas…) o el simple mantenimiento en páginas web ajenas, sin consentimiento del titular, sin necesidad de móvil o acción posterior alguna, y se castiga con pena de hasta dos años. Se castiga, pues, el mero hecho de saltarse las barreras de seguridad informáticas, como un atentado al derecho a la "intimidad informática" pero siempre que exista un acceso a los datos o programas albergados». O la SAP de Madrid sec 7 nº. 895/2017, de 27 noviembre (ECLI:ES:APM:2017:16438), estima que «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 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"».

25 Comparten esta concepción del bien jurídico del delito tipificado en el art. 264 bis del Código penal Benítez Ortúzar, *Sistema de Derecho penal, Parte Especial,* 2ª ed., Morillas Cueva Dir., Dykinson, Madrid, 2016, p. 611; Mestre Delgado, *Delitos, La parte especial del Derecho penal,* 3ª ed., Lamarca Pérez coord., Colex, Madrid, 2015, pp. 390 y ss. Muñoz Conde, *Derecho penal, Parte Especial*, 22ª ed., pp. 433 y 434 indica que el delito de daños supone que se disminuya el valor de la cosa dañada, lesionando su esencia o sustancia y añade que la cosa dañada debe tener algún valor patrimonial económicamente valorable. En relación con el delito tipificado en el art. 264 bis del Código penal señala que el concepto de daño incluye la afectación de la posibilidad de uso del objeto material sobre el que recae la acción y conlleva un daño patrimonial; véase el mismo, ob. cit., p. 420. López Gorostidi, «Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: apropósito del confinamiento provocado por la crisis sanitaria del COVID-19», p. 146.

26 Véanse Lucena Cid, «El concepto de la intimidad en los nuevos contextos tecnológicos», pp. 33 y ss.; Ribagorda Garnacho, «Seguridad de las tecnologías de la información», p. 310. Estas estructuras y relaciones se pueden mantener mediante diversos dispositivos o canales que aún no están disponibles hoy en día.

27 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4625. Sobre la ubicación sistemática de estos comportamientos delictivos en el marco de los delitos patrimoniales, véase Miró LLinares, ob. cit., marginal 4629.

28 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4630. Manifiesta que el legislador debería haber aprovechado la última reforma del Código penal para integrar los delitos que tienen como referencia "daños informáticos" en un capítulo o sección diferente para «romper definitivamente» las ligaduras interpretativas que acompañan al delito común de daños y que son de difícil encaje en las figuras delictivas de los arts. 264 y 264 bis del Código penal. Véase también Miró LLinares, *El cibercrimen,* pp. 65 y 66.

29 El § 303b del StGB dispone que «1. El que interfiera de manera relevante en un procesamiento de datos que es de significado esencial para un tercero, de modo que 1) comete el hecho tipificado en el § 303a; 2) introduce o transmite datos (en el sentido del § 202a) con la intención de causar un perjuicio a otro; o 3) destroce, dañe, destruye, inutilice, elimine o modifique un sistema de procesamiento de datos o un soporte de datos, será castigado con una pena privativa de libertad de hasta tres años o con pena de multa. 2. Si el proce-

go, me parece más apropiado destacar los aspectos más esenciales de los sistemas de información y de comunicación, la confidencialidad, la integridad y la disponibilidad, que explican que dichos sistemas ejecuten las diversas funciones que tienen, dependiendo del medio concreto (económico, social, administrativo, laboral, sanitario, etc.) en el que se desarrollen y proporcionen su utilidad social.

El objeto de protección que hemos indicado —la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos— se encuentra expresado en el preámbulo del Convenio del Consejo de Europa sobre Cibercriminalidad, donde se pone de relieve la necesidad de «prevenir las acciones que suponen un atentado a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos, así como el uso fraudulento de tales sistemas, redes y datos, velando por la incriminación de aquellos comportamientos descritos en el presente convenio». Asimismo en la Directiva (UE) 2016/1148 del Parlamento europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, se define en el art. 4 la seguridad de las redes y sistemas de información como «la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos». Además, estudios técnicos sobre seguridad informática recogen también la necesidad de proteger la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos[30]. Desde mi punto de vista esta es la línea adecuada para definir el bien jurídico protegido en la criminalización de los ataques contra los sistemas de información y de comunicación, si bien es cierto que es necesario distinguir, por un lado, la confidencialidad, la integridad y la disponibilidad de los sistemas de información y, por otro lado, de los datos propiamente dichos. En nuestro Código penal ya se protege la obtención, la utilización o modificación de los datos que se almacenen en un sistema informático mediante diversos tipos delictivos en función de la naturaleza de tales datos (arts. 197, 200, 248, 255, 264, 270, 278 o 598 del Código penal), lo que parece sistemáticamente más correcto. Ahora, sin embargo, nos vamos a centrar, exclusivamente en la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, entendiendo por tales, como se indica en el artículo 1 del Convenio del Consejo de Europa sobre Cibercriminalidad «a todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, al ejecutar un programa, el tratamiento automatizado de datos». A continuación, indagaremos tanto en la necesidad de la existencia de este bien jurídico protegido como en su autonomía.

El Derecho Penal es un sector del ordenamiento jurídico que tiene encomendada la misión de proteger los bienes vitales fundamentales del individuo y la comunidad, los cuales son elevados por la protección de las normas del Derecho a la categoría de bienes jurídicos[31]. Los bienes jurídicos no tienen una entidad material o

samiento de datos es de significación esencial para un negocio o empresa de terceros o una Administración pública, la pena será privativa de libertad de hasta cinco años o pena de multa. 3. La tentativa es punible. 4. En casos particularmente graves del párrafo 2 la pena es privativa de libertad de seis meses a diez años. Un caso particularmente grave suele ser cuando el autor 1) causa un perjuicio de grandes dimensiones, 2) actúa profesionalmente o como miembro de una organización, a la que se ha unido para cometer de manera continuada sabotaje informático, 3) perjudique a través del hecho el suministro de bienes o servicios vitales a la población o la seguridad de la República Federal de Alemania. 5. A los actos preparatorios del hecho punible previsto en el párrafo 1 se aplica consecuentemente el § 202c». El § 303a que castiga las "intervenciones sobre los datos" dispone que «1. El que borre, suprima, inutilice o modifique datos (§ 202 a 2) de manera ilícita, será castigado con una pena de prisión de hasta dos años o una multa. 2. La tentativa es punible. 3. A los actos preparatorios del hecho punible previsto en el párrafo 1 se aplica consecuentemente el § 202c». El § 202a del StGB que tipifica el delito de "espionaje de datos" establece que «1. El que ilícitamente se procura el acceso a datos para sí o un tercero, que no le están destinados y que están especialmente protegidos contra un acceso no autorizado, vulnerando las barreras de seguridad, será castigado con una pena de prisión de hasta tres años o una multa. 2. Datos en el sentido del párrafo anterior son solo aquellos que son transmitidos o almacenados de manera electrónica, magnética o de otro modo no directamente perceptible».

Sobre este bien jurídico protegido en este delito, véanse Möhrenschlager, «Das neue Computerstrafrecht», Wistra, 1986, p. 142; Lackner/Kühl, «§ 303b», *Strafgesetzbuch Kommentar*, 29 Auflage, Rn. 1; Wolf, «§ 303b», Strafgesetzbuch. Leipziger Kommentar Großkommentar, 12 Auflage, Rn. 2; Stree/Hecker, *Schönke/Schröder, Strafgesetzbuch Kommentar*, 30 Auflage, Rn. 1; Zaczyk, «§ 303b», Nomos-Kommentar Strafgesetzbuch, 5 Auflage, Rn. 1; Hoyer, «§ 303b», SK-StGB, Rn. 2 y 3 en relación con el § 303b párrafo 2. No obstante, sostiene que el patrimonio es el bien jurídico protegido en el delito de Computersabotage del § 303b del StGB Fischer, *Strafgesetzbuch mit Nebengesetzen Kommentar*, 67 Auflage, § 303b, Rn. 2.

30 Véanse Ribagorda Garnacho, «Seguridad de las tecnologías de la información», pp. 307 y ss.; Longstaff/Ellis/Hernan/Lipson/McMillan/Pesante/Simmel, «Security of the Internet», pp. 231-255.

31 Véase Cerezo Mir, Curso de Derecho penal español, Parte General, I. Introducción, 6ª ed., p. 13. Véase una reciente exposición de las diversas concepciones del bien jurídico en la actualidad en la obra de Pérez-Sauquillo Muñoz, *Legitimidad y técnicas de protección penal de bienes jurídicos supraindividuales*, pp. 40 y ss.

física, sino que, por el contrario, son valores ideales que se atribuyen por la comunidad social a determinados objetos, cosas, situaciones o relaciones en virtud de su aptitud e idoneidad instrumental para la satisfacción de necesidades individuales y colectivas[32]. Estas necesidades y los intereses que satisfacen ya sean individuales o colectivos son además plurales, variados y, a menudo, también contrapuestos. Sin embargo, el bien jurídico debe ser una entidad libre de conflictos y antagonismos, pues en cuanto instrumento social y políticamente sancionado y dispuesto para la satisfacción de necesidades e intereses plurales[33], el bien jurídico, como afirma Bustos Ramírez, surge como una síntesis normativa (fijada por el ordenamiento jurídico) de una relación social determinada y dinámica[34]. Lo que interesa salvaguardar, entonces, son las relaciones sociales mismas, la posición concreta que en ella ocupan los individuos, su intermediación con objetos y entes, y sus transformaciones por la interacción social. Los bienes jurídicos, concluye Bustos Ramírez, lo que hacen es plasmar de una forma concreta este complejo real social que interesa proteger[35].

Los bienes jurídicos configuran un espacio social que delimita, a su vez, las condiciones necesarias para que otros bienes jurídicos involucrados en dicho espacio, se desenvuelvan correctamente. Cuando estas condiciones necesarias para el desenvolvimiento correcto de los bienes jurídicos se desarrollan con normalidad, posibilitan a los bienes unas mayores posibilidades de rendimiento y aprovechamiento. La normalidad en el desarrollo de estas condiciones necesarias puede, incluso, acarrear la subordinación absoluta de un bien jurídico al cumplimiento de la función social de otro[36]. En este espacio social se puede constatar la existencia de dos clases de bienes jurídicos.

a) Por un lado, existen unos bienes jurídicos de corte clásico cuyas notas más importantes son su fácil determinación, su directa vinculación a la persona en sus relaciones específicas de modo que afectan a las bases mismas de existencia del sistema social, esto es, a las personas y están referidos a las relaciones de una persona con otra, de ahí que sean de tan fácil y elemental delimitación[37]. Estos bienes jurídicos, con carácter general, no admiten quedar involucrados en el quehacer cotidiano de las relaciones sociales y este es el motivo por el que sus afecciones suelen ser de carácter estrictamente personal y puntual[38]. En efecto, la vida, la intimidad personal y familiar o el patrimonio son bienes jurídicos que responden a tales características y que se denominan bienes jurídicos individuales.

b) No obstante, por el dinamismo que ha adquirido la sociedad moderna se han ido configurando unos bienes jurídicos que presentan múltiples dificultades para su determinación y que han recibido la denominación de

32 A los efectos que aquí nos interesan acogemos la noción de necesidad de Terradillos Basoco para quien «las necesidades son expresión de valores y cuanto más universales sean éstos, más radicales serán aquéllas. De otro modo no tendría ningún sentido acudir a este criterio que llevaría a un burdo utilitarismo afectado por las mismas limitaciones que las inherentes a la idea de interés. Pero parece atractivo tomar a la necesidad como punto de referencia, pues ello nos permite, de entrada, eliminar los riesgos de postergación del individuo… o de utilización ético-ideológica del Derecho penal… El concepto de necesidad contiene además elementos de generalidad y contrastabilidad que le hacen especialmente apto para ser la base de un discurso racional». Véase Terradillos Basoco, «La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal», p. 137. Más adelante concluye que «una política criminal alternativa que pretenda no ser autoritaria ha de limitarse, hoy, a la defensa, de las posibilidades reales de participación igualitaria y ha de tender, por ello, a la satisfacción del máximo de necesidades del máximo número de ciudadanos»; véase el mismo, ob. cit., p. 140.

33 Véase la noción de necesidad en este contexto desarrollada por Terradillos Basoco, «La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal», pp. 136 y ss., siguiendo a A. Heller.

34 Véanse Bustos Ramírez, «Del estado actual de la teoría del injusto», p. 138; Bustos Ramírez/Hormazábal Malarée, *Lecciones de Derecho penal, Parte General*, pp. 71 y ss.

35 Véase Bustos Ramírez, «Política criminal e injusto. (Política criminal, bien jurídico, desvalor de acto y de resultado)», p.166.

36 Véase sobre estas tesis, más ampliamente, Gracia Martín, Fundamentos de dogmática penal. Una introducción a la concepción finalista de la responsabilidad penal, pp. 215 y ss., 216 y ss, 224 y ss.

37 Véase Bustos Ramírez, «Perspectivas actuales del Derecho Penal Económico», pp. 213 y 214.

38 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 158. Naturalmente determinados bienes jurídicos, ya sean estos individuales o colectivos, pueden resultar afectados al encontrarse involucrados de un modo consustancial en una actividad social valorada positivamente por la utilidad general que reporta. Estas afecciones no constituyen un desvalor penal del resultado porque son socialmente adecuadas. Sobre esta tesis, véanse, Rueda Martín, *La teoría de la imputación objetiva del resultado en el delito doloso de acción. (Una investigación, a la vez, sobre los límites ontológicos de las valoraciones jurídico-penales en el ámbito de lo injusto),* pp. 247 y ss., 251 y ss., 278 y ss.; Gracia Martín, «El finalismo como método sintético real-normativo para la construcción de la teoría del delito», pp. 17 y ss.

"bienes jurídicos colectivos"[39]. Una nota característica de estos bienes jurídicos, entre otras[40], es que éstos están ligados al funcionamiento del sistema ya que no se trata sólo de relaciones sociales básicas dentro del sistema y configuradoras del orden social[41]. Ahora bien, estos bienes jurídicos no constituyen una categoría que está por encima del individuo o que va más allá de él, sino que hay «que definirlos a partir de una relación social basada en la satisfacción de necesidades de cada uno de los miembros de la sociedad o de un colectivo y en conformidad con el funcionamiento del sistema social»[42]. Este grupo de bienes jurídicos aparecen como complementarios, desde una perspectiva material, de otros bienes jurídicos que no tienen que ser, exclusivamente, individuales; es decir, tienen que prestar una serie de utilidades a otros bienes jurídicos[43]. La función de los bienes jurídicos colectivos, de prestar utilidades a otros bienes jurídicos, a juicio de Gracia Martín, se bifurca en dos direcciones, de modo que podemos hablar de una doble función según que contemplemos los aspectos de ésta que podemos llamar, respectivamente, negativa y positiva[44]. Por un lado, hay que destacar una función negativa de contención de riesgos para determinados bienes jurídicos reconocida, unánimemente de forma implícita o explícita, en la doctrina lo que explica su relación de complementariedad[45]. Por otro lado, existe asimismo una función positiva de creación y configuración de espacios que delimiten las condiciones en las que los bienes jurídicos a los que complementan pueden cumplir realmente una función social para todos los ciudadanos y que les dota de autonomía[46]. Ambas funciones están estrechamente entrelazadas y sólo por razones expositivas se distinguen. Tampoco debe olvidarse que una vez reconocido por el ordenamiento un bien jurídico colectivo, con carácter general, debe admitirse su independencia y su posibilidad de lesión sin necesidad de exigir un efecto simultáneo sobre bienes jurídicos individuales.

El bien jurídico aludido y que se refiere a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos constituye una barrera de contención de riesgos para otros bienes jurídicos que se puedan encontrar involucrados en la función social que desempeñen tales sistemas y redes informáticos, como sucede con la intimidad personal y familiar, el patrimonio, etc[47].. Así, por ejemplo, el bien jurídico intimidad

39 Se ha optado por esta denominación bastante utilizada en la doctrina frente a otras denominaciones porque, como indica Soto Navarro, el adjetivo "colectivo" denota la dualidad de "ser perteneciente o relativo a cualquier agrupación de individuos"; véase Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna,* pp. 193 y 194.

40 Sobre las características de los bienes jurídicos colectivos, véase el estudio de Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna,* pp. 193 y ss. Sobre las características de los bienes jurídicos colectivos, véanse, entre otros, los estudios de Santana Vega, *La protección penal de los bienes jurídicos colectivos*, *passim*; Hefendehl, *Grund un Grenzen des Schutzes kollektiver Rechtsgüter im Strafrecht*, passim*;* Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna*, *passim* y Pérez-Sauquillo Muñoz, *Legitimidad y técnicas de protección penal de bienes jurídicos supraindividuales*, *passim*.

41 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 158.

42 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 159.

43 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», p. 159. Este autor, sin embargo, se refiere a la relación de complementariedad entre los bienes jurídicos individuales y los colectivos. A mi juicio dicha relación de complementariedad se establece con carácter general entre los bienes jurídicos colectivos y otros bienes jurídicos ya sean individuales o colectivos.

Una consecuencia de esta nota de los bienes jurídicos colectivos es la vertiente positiva del carácter indisponible de dichos bienes jurídicos, contemplada como la posibilidad de aprovechamiento por todos, sin que nadie pueda ser excluido y sin que el aprovechamiento individual obstaculice ni impida el aprovechamiento por otros; véase Hefendehl, *Grund un Grenzen des Schutzes kollektiver Rechtsgüter im Strafrecht,* pp. 21, 126-128.

44 Véase Gracia Martín, «Nuevas perspectivas del Derecho penal tributario. (Las "funciones del tributo" como bien jurídico)», pp. 210 y 211. En la p. 211, nota 103, pone como ejemplo de bien jurídico colectivo la seguridad e higiene en el trabajo, pues no sólo cumple una función negativa de contención de riesgos para los bienes vida, integridad física y salud, sino la positiva de delimitar un espacio social en que dichos bienes más allá de su existencia material alcancen la calidad adecuada a la dignidad humana.

45 Véase Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», pp. 158 y ss.

46 La doctrina mayoritaria se pronuncia a favor de la autonomía de los bienes jurídicos colectivos. Como ha afirmado Soto Navarro la función social de los bienes jurídicos colectivos permite conceptuarlos de forma autónoma; véase Soto Navarro, *La protección penal de los bienes colectivos en la sociedad moderna,* p. 231. También, aunque de una forma matizada Pérez-Sauquillo Muñoz, *Legitimidad y técnicas de protección penal de bienes jurídicos supraindividuales*, pp. 102 y ss.

47 En relación con el bien jurídico definido como la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, Mourullo, Alonso y Lascuraín apuntan que éste «tiene un carácter instrumental con respecto a otros intereses jurídicamente relevantes, sean éstos objeto directo de protección por el derecho penal o no»; véanse Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez,

personal y familiar puede encontrarse involucrado en la función social que desempeña el bien jurídico relativo a la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos. Con respecto al bien jurídico intimidad personal y familiar, el Código penal organiza un sistema de tipos delictivos recogidos en el art. 197. En el apartado 2º de este tipo delictivo[48], la protección penal de la intimidad personal y familiar se lleva a cabo a través de unas acciones consistentes, por una parte, en el acceso y la alteración o, por otra parte, en el acceso y la utilización de los datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado por parte de una persona no autorizada, de manera que se realizará la conducta típica del art. 197.2 del Código penal siempre y cuando se actúe "en perjuicio del titular de los datos o de un tercero". Estas conductas lesionan el bien jurídico intimidad personal y familiar de una típicamente relevante[49], pero también hay que constatar que con tales comportamientos se produce la lesión de la confidencialidad, integridad y disponibilidad de los sistemas informáticos mediante el simple acceso a los mismos, tanto si se realiza en perjuicio del titular de los datos o de un tercero como si se realiza con la finalidad de descubrir fallos o puertas falsas en dichos sistemas informáticos que albergan archivos de datos reservados. Si se registran unos datos reservados de carácter personal o familiar de una persona en un fichero telemático, la protección del bien jurídico intimidad personal y familiar se reforzará y se asegurará si se protege penalmente la confidencialidad, la integridad y la disponibilidad del sistema que albergue dicho fichero. Lo mismo sucede respecto al bien jurídico relativo a la capacidad competitiva de la empresa, dada la posición ventajosa en las relaciones del tráfico económico que ostenta el titular de la información, entendida como valor económico, protegido en el art. 278.1 del Código penal [50], el patrimonio protegido en el art. 264.1[51] del Código penal o incluso la seguridad y/o

«Derecho penal e internet», p. 261. Véase también la exposición realizada en la p. 269. Por otra parte, Carrasco Andrino, *Derecho penal español, Parte Especial (I)*, 2ª ed., p. 783 destaca asimismo que el aludido bien jurídico funciona como una barrera de contención de riesgos para otros intereses relevantes (intimidad, patrimonio, seguridad nacional, etc., adquiriendo su protección un carácter instrumental).

La tesis que sostiene que los bienes jurídicos colectivos suponen una barrera de contención de riesgos para bienes jurídicos individuales se encuentra expresada por la doctrina, cuando afirma en relación con determinados delitos que suponen un adelantamiento de las barreras de protección de dichos bienes jurídicos individuales. Por ejemplo, Bolea Bardon, *Comentarios al Código penal*, p. 744 indica sobre el bien jurídico protegido en el art. 197 bis que «frente a la tesis que sostiene que el bien jurídico protegido en este delito es la seguridad de los sistemas informáticos, cabe defender que la incriminación de esta conducta supone un adelantamiento de las barreras de protección de la intimidad que parte de la consideración de que la mera intromisión informática pone en peligro la privacidad del titular del sistema». De forma similar Anarte Borrallo/Doval País, *Derecho penal, Parte Especial,* 2ª ed., p. 513; Queralt Jiménez, *Derecho penal español, Parte Especial*, 7ª ed., p. 313; Miró LLinares, «Delitos informáticos. Hacking. Daños», marginal nº. 1438, quien concluye que «la tipificación del *hacking* supone una anticipación de las barreras de protección de la intimidad, puesto que la mera intromisión informática ya pone en *riesgo la privacidad del titular del sistema*… En este sentido, la tipificación del "*hacking*" también supondrá un adelantamiento de las barreras de protección del patrimonio, puesto que con ella se está castigando un acto preparatorio previo para la lesión del bien jurídico». En un sentido parecido Matellanes Rodríguez, «Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)», p. 66.

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

49 Véase Rueda Martín, *Protección penal de la intimidad personal e informática,* p. 77. En este ejemplo, en la medida que se encuentra involucrado el bien jurídico intimidad personal y familiar en estos comportamientos a través de la alteración de los datos reservados contenidos en ese sistema informático, el simple acceso al sistema informático constituirá una tentativa del art. 197.2 del Código penal, si concurre el elemento subjetivo de lo injusto indicado.

50 Véase Mayo Calderón, *Derecho penal, Parte Especial*, p. 411.

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

51 El art. 264.1 del Código penal establece que «El que por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años». Respecto del bien jurídico protegido en el citado precepto es necesario indicar que hay una discusión doctrinal, ya que entre otras opiniones un sector estima que es el objeto de protección es el patrimonio [véanse, por ejemplo, Navarro Frías, Derecho penal, Parte Especial, p. 390; González Rus, «Daños a través de internet y denegación de servicios», p. 1471; Mata y Martín, *Delincuencia informática y Derecho penal*, pp. 77 y ss.;

defensa nacional en relación con el art. 598 del Código penal[52]. Los mencionados bienes jurídicos se verán más protegidos en tanto en cuanto se garantice la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos en los que se involucren[53]. Este bien jurídico actúa como una barrera de contención de riesgos para otros bienes jurídicos como los citados. Ahora bien, como se ha indicado antes, para que un objeto, situación o relación adquiera la categoría de bien jurídico colectivo es preciso que, además de esa función negativa de contención de riesgos, cumpla una función positiva de creación y configuración de espacios que delimiten las condiciones en que los bienes jurídicos a los que complementan puedan cumplir realmente su función social[54]. Vamos a analizar a continuación si el bien jurídico que estamos estudiando desarrolla esta función positiva.

Si nos detenemos en el funcionamiento del sistema social en la actualidad es innegable la importancia que han adquirido las TIC, con la utilización de redes y sistemas de tratamiento de la información, como medio de crecimiento económico y desarrollo social[55]. Las TIC se han extendido y se han enraizado en nuestras modernas sociedades de tal manera que, como hemos indicado, 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 ha permitido la aparición de nuevos escenarios como, por ejemplo, el comercio electrónico (*e-commerce*), el acercamiento de los bancos a los clientes (*home-banking),* la gestión electrónica de los recursos de las empresas (*e-management*), la gestión doméstica (*domótica*)[56] o la tramitación electrónica entre la ciudadanía y las Administraciones Públicas, que sirve mejor a los principios de eficacia y eficiencia y refuerza las garantías de los interesados, como dispone la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas, en cuya Exposición de Motivos, se dispone que «el desarrollo de las tecnologías de la información y comunicación también ha venido afectando profundamente a la forma y al contenido de las relaciones de la Administración con los ciudadanos y las empresas. Si bien la Ley 30/1992, de 26 de noviembre, ya fue consciente del impacto de las nuevas tecnologías en las relaciones administrativas, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, les otorgó carta de naturaleza legal, al establecer el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y sistemas necesarios para que ese derecho pudiera ejercerse. Sin embargo, en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos, sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados». En estos escenarios enmarcados en la utilización de las TIC se involucran bienes jurídicos tales como el patrimonio, la intimidad personal y familiar o la capacidad competitiva de la empresa, de manera que los sistemas de información permiten su desarrollo en las modernas sociedades.

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

Muñoz Conde, *Derecho penal, Parte Especial*, 22ª ed., pp. 433, 434 y 438], mientras que otro sector considera que se protege la integridad o disponibilidad de los datos y sistemas informáticos [véanse, por ejemplo, Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e internet», pp. 282 y ss.].

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

53 Véase Miró LLinares, «Delitos informáticos. Hacking. Daños», marginal nº. 1438.

54 Véase Gracia Martín, «Nuevas perspectivas del Derecho penal tributario. (Las "funciones del tributo" como bien jurídico)», pp. 210-211.

55 Véanse Romeo Casabona, *Poder informático y seguridad jurídica. La función tutelar del derecho penal ante las Nuevas Tecnologías de la Información,* pp. 19 y ss.; Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», pp. 250 y 274. Al comienzo de la Exposición de Motivos de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE de 23 de junio de 2007), se indica que «las tecnologías de la información y las comunicaciones están afectando también muy profundamente a la forma e incluso al contenido de las relaciones de los seres humanos entre sí y de las sociedades en que se integran».

56 Véase Salom Clotet, «Delito informático y su investigación», pp. 93 y ss.

por lo que de los riesgos que se derivan de su vulnerabilidad[57] ha surgido, consecuentemente, un interés en la seguridad de la utilización de las TIC. En el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, se indica en su Preámbulo que «la evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales. Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis»[58]. En la exposición de motivos del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, también se pone de manifiesto que «la Estrategia de Seguridad Nacional 2017, aprobada mediante Real Decreto 1008/2017, de 1 de diciembre, identifica las ciberamenazas y el espionaje como amenazas que comprometen o socavan la seguridad nacional y, en coherencia con ello, singulariza la ciberseguridad como uno de sus ámbitos prioritarios de actuación. El desarrollo tecnológico implica una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos e información, el hackeo de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas. La hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública y exige una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano».

En consecuencia, el Derecho cuando protege las TIC reconoce su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. La necesidad de proteger los sistemas de comunicación e información por dicho valor social se ha reconocido también en la STC alemán de 27 de febrero de 2008 que establece en su parágrafo nº. 181 que: «c) De la importancia de la utilización de los sistemas tecnológicos de información para el desarrollo de la personalidad y de los peligros para la misma unidos a dicha utilización, resulta una importante necesidad de protección desde el punto de vista de los derechos fundamentales. Los particulares exigen que el Estado atienda las expectativas de confidencialidad e integridad de tales sistemas justificadas en el marco del libre desarrollo de la personalidad». Y, posteriormente, en el parágrafo 203 afirma que: «Por otra parte, el derecho fundamental a la garantía de la integridad y confidencialidad de los sistemas tecnológicos de información hay que esgrimirlo cuando la facultad de injerencia afecte a un sistema, que por sí solo o en conexión con redes tecnológicas, en un contorno cerrado o amplio, pueda contener datos del afectado referentes a su persona, de modo que el acceso al sistema permitiría formarse una idea sobre aspectos esenciales de la vida de una persona o incluso obtener una imagen representativa de su personalidad»[59].

57 Rodríguez Mourullo, Alonso Gallo, Lascuraín Sánchez señalan asimismo que «los estudios doctrinales y los informes de agencias internacionales y de organizaciones públicas y privadas han advertido una y otra vez sobre los riesgos derivados de la vulnerabilidad de unos sistemas y redes informáticos de los que toda la organización social (el sistema financiero, las infraestructuras básicas, las empresas, los organismos públicos, los particulares) ha pasado a depender de forma extraordinaria»; véanse los mismos, «Derecho penal e internet», p. 257.

58 Recordando lo que se establecía en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, ya derogada, para garantizar la comunicación y la relación electrónica entre los ciudadanos con las Administraciones Públicas se tiene que asegurar la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias. Asimismo, se deben crear las condiciones de confianza en el uso de medios electrónicos, contemplando las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos. En dicha Ley se establecía en el art. 1.2 que «*las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias*». Asimismo en el art. 3.3 se disponía como fin de la mencionada Ley, *«crear las condiciones de confianza en el uso de medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos*». También se contemplaba como uno de sus principios generales en el art. 4, f) el «principio de seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas».

59 Véase la STC alemán de 27 de febrero de 2008 —BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 -1 BvR 370/07- Rn. (1-333)—, disponible en la dirección http://www.bverfg.de/e/rs20080227_1bvr037007.html.

La utilización de las TIC en los ámbitos reseñados ha conducido al surgimiento de unos intereses que tienen unas notas comunes[60]. 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[61], como un instrumento que facilita sus relaciones sociales, económicas, etc. También las empresas tienen en los modernos sistemas informáticos un instrumento que facilita y potencia su actividad económica y que supone una notable ventaja competitiva en el mercado[62], y tienen interés en que se proteja no sólo el contenido de la información que almacenan, sino además la confidencialidad y la integridad de dicho sistema. Del mismo modo, los organismos públicos tienen interés en la protección de los sistemas informáticos que almacenan los datos personales de todo tipo o que regulan las relaciones de las distintas administraciones con los administrados, fundamental para el debido funcionamiento de estas[63]. Además de este interés generalizado debemos observar que la realización de diversas operaciones económicas, financieras, empresariales, laborales, administrativas, etc. por parte de los usuarios tiene que llevarse a cabo de una forma práctica pero segura, es decir, garantizando tanto la disponibilidad del sistema informático como la identidad o la autenticación de la persona que accede a dicho sistema. Los usuarios (administrados, empresas, etc.) tienen interés en que cumpliendo unos determinados requisitos se pueda acceder a dichos sistemas informáticos para llevar a cabo aquellas operaciones que sean relevantes, sin que se interpongan demasiados obstáculos. En suma nos encontramos con la convergencia de todos estos intereses que explican, por una parte, la función social de los sistemas de información como importantes herramientas de crecimiento y desarrollo económico y social; y, por otra parte, explican la demanda de medidas de seguridad de carácter técnico y de organización en su utilización, que incluyen mecanismos y prácticas profesionales que permiten tanto un uso continuado de las tecnologías como el establecimiento de acciones destinadas a interrumpir o sabotear su funcionamiento o la interpretación de datos elaborados y tratados por otros[64].

Esta seguridad en la utilización de los sistemas informáticos de forma más o menos generalizada se manifiesta en la confidencialidad, integridad y la disponibilidad de los sistemas de comunicación e información[65], y que constituye propiamente el bien jurídico a proteger en la criminalización de determinados ataques contra los sistemas de información. La integridad de un sistema informático alude a su utilización con las pertinentes modificaciones del contenido de la información almacenada en el sistema por parte de la/s persona/s autorizada/s. La confidencialidad de dicho sistema se basa en que su utilización corresponde exclusivamente a la/s persona/s autorizada/s. La disponibilidad hace referencia al control sobre la utilización de un determinado sistema por parte de la/s persona/s autorizada/s. El bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información merece la protección del ordenamiento jurídico y dada la importante función social que desempeña, se legitima la intervención del Derecho penal en su protección, así

60 En la STC alemán de 27 de febrero de 2008 —BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 -1 BvR 370/07- Rn. (1-333)— en su parágrafo 204 disponible en la dirección http://www.bverfg.de/e/rs20080227_1bvr037007.html, se reconoce también con carácter general el interés de los interesados que utilizan sistemas tecnológicos de información en garantizar la confidencialidad e integridad de dichos sistemas. Véanse también Miró LLinares, *El cibercrimen*, pp. 52 y ss.; Gómez Vieites, *Seguridad en equipos informáticos*, pp. 25 y ss.

61 Véanse Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», p. 301; Matellanes Rodríguez, «Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)», p. 65.

62 Véase Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», p. 274, quien destaca que la informatización para las empresas implica contabilidades, carteras de clientes, balances, informes y proyectos empresariales, estrategias de mercado, procedimientos económicos o tecnológicos de carácter reservado, o datos de investigación y desarrollo de tecnología.

63 Destacan la protección de los intereses de la economía y la administración pública en la funcionalidad del procesamiento de datos en el delito de Computersabotage del § 303b del StGB: Lackner/Kühl, «§ 303b», *Strafgesetzbuch Kommentar*, 29 Auflage, Rn. 1; Hoyer, «§ 303b», SK-StGB, Rn. 2 y 3 en relación con el § 303b párrafo 2; Stree/Hecker, *Schönke/Schröder, Strafgesetzbuch Kommentar*, 30 Auflage, Rn. 1; Wolf, *Strafgesetzbuch. Leipziger Kommentar Großkommentar*, 12 Auflage, Rn. 2; Möhrenschlager, «Das neue Computerstrafrecht», p. 142; Nemzov, *Strafbarkeit von Online-Blockaden und DDoS-Angriffen*, p. 111; Schulze-Heiming, Der strafrechtliche Schutz von Computerdaten gegen die Angriffsformen ser Spionage, Sabotage und des Zeitdiebstahls, p. 195.

64 Sobre esta demanda de medidas de seguridad de carácter técnico y de organización, véase Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 48. En cuanto a las medidas de seguridad, desde un punto de vista técnico, véase la exposición realizada por Huidobro Moya/Roldán Martínez, *Seguridad en redes y sistemas informáticos*, *passim*; Ribagorda Garnacho, «La protección de datos personales y la seguridad de la información», pp. 381 y ss.; Gómez Vieites, *Seguridad en equipos informáticos*, pp. 78 y ss.

65 Véase Ribagorda Garnacho, «Seguridad de las tecnologías de la información», pp. 312 y 313; Gómez Vieites, *Seguridad en equipos informáticos*, pp. 20 y ss.; Costas Sanchos, *Seguridad informática*, pp. 21 y ss.

como en la represión de aquellos comportamientos que lo lesionen[66].

Una vez fundamentada la existencia y la autonomía del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos, debemos exponer argumentos que justifiquen la necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión del bien jurídico estudiado. En primer lugar, cabe destacar la importancia de proteger penalmente y no sólo administrativamente la función social que desempeña el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos. Ya hemos explicado que nuestra organización social (la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, los particulares, etc.) ha pasado a depender de forma extraordinaria de la utilización de unos sistemas y redes informáticos, como medio de crecimiento económico y desarrollo social. En los últimos años el Derecho ha desplegado una regulación y protección de las nuevas tecnologías de la información, y ha reconocido su valor social positivo como necesario y vinculante para un correcto funcionamiento del sistema social. Consecuentemente ha surgido también un interés en la seguridad de la utilización de las TIC desde diversos ámbitos, que se concreta en la confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido dotado de autonomía y que, además, sirve de barrera de contención de riesgos para otros bienes jurídicos que puedan verse implicados en la utilización de sistemas y redes informáticos. En segundo lugar, elevar a la categoría de delito en nuestro Código penal esta clase comportamientos que supongan un ataque contra los sistemas de comunicación o información, supone una obligada armonización penal en este ámbito de nuestra legislación con lo dispuesto en otros estados de la Unión Europea, en consonancia con lo establecido en el Reglamento (UE) 2019/796, en la Directiva 2013/40/UE, y en el Convenio del Consejo de Europa sobre Cibercriminalidad. Dicha armonización es necesaria además porque en esta clase de ataques podemos encontrar una nota que le añade un especial grado de peligrosidad: su conexión internacional o transfronteriza, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto, y resulta sorprendente que en algún territorio un ataque contra un sistema informático pueda resultar impune[67]. En tercer lugar, hay que tener en cuenta que, como afirma Romeo Casabona, el ciberespacio presenta unos perfiles de gran interés para el Derecho penal entre los que destaca la potencialidad multiplicadora de las acciones ilícitas y de sus efectos lesivos para los bienes jurídicos afectados[68]. Esta característica se puede apreciar con especial intensidad no solo en las conductas de acceso ilícito a sistemas informáticos, sino también en las que producen una denegación de servicios, que como ha puesto de relieve un sector doctrinal tienen un efecto criminógeno[69]. Por ello y con carácter general, el ciberespacio se presenta en las sociedades modernas como una de las posibles fuentes de riesgos necesitados de control, y dada la gravedad de sus repercusiones sobre diferentes bienes jurídicos que se tienen que involucrar en dicho espacio se legitima la intervención del Derecho penal.

IV. OPCIONES POLÍTICO CRIMINALES PARA TIPIFICAR LOS ATAQUES DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN

Una vez que hemos fundamentado la necesidad político-criminal de criminalizar aquellas conductas que supongan una lesión del bien jurídico estudiado, debemos plantearnos qué opciones tiene a su disposición el

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

67 Véase sobre esta necesidad De la Mata Barranco, Derecho penal europeo y legislación española: las reformas del Código penal. Actualizado a la reforma penal 2015, pp. 71 y ss.

68 Véase Romeo Casabona, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», p. 4. También destacan, con carácter general, el factor criminógeno del procesamiento electrónico de datos, Sieber, *Computerkriminalität*, 1ª ed., pp. 158 y ss.; Mata y Martín, *Delincuencia informática y Derecho penal,* p. 17, 24 y ss.; Morón Lerma, *Internet y Derecho penal: Hacking y otras conductas ilícitas en la red*, p. 75.

69 Véase respecto de las conductas de hacking, Gutiérrez Francés, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», pp. 1179 y ss.; la misma, «Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa», p. 206.

legislador para criminalizar aquellas conductas que lo lesionen o lo pongan en peligro[70]. En primer lugar, el legislador puede establecer tipos específicos o «tipos de equivalencia», que contemplen la incriminación de determinados ataques contra los sistemas de información en cada figura de delito particular, con el fin de suplir las posibles lagunas de punibilidad que pudieran evidenciarse. Esta es una técnica de tipificación adoptada en algunos Códigos penales europeos. A mero título de ejemplo, en el Código penal alemán se castiga en el primer párrafo del § 202a, dentro de la sección dedicada a los ataques a la vida privada y la confidencialidad, a «quien sin autorización se procura datos para sí o un tercero, que no le están destinados y que están especialmente protegidos contra un acceso no autorizado, vulnerando las barreras de acceso», con una pena de prisión de hasta tres años o una multa. En el segundo párrafo del § 202a se aclara que «Datos en el sentido del párrafo 1 son solo aquellos que se almacenan o transmiten electrónicamente, magnéticamente o de otra manera no perceptible». En el § 202b se penaliza la interceptación de datos: «Quien ilícitamente obtenga datos (los del 202a segundo párrafo) para sí o un tercero, no destinados a él con la utilización de medios técnicos a través de una transmisión de datos no pública o de la radiación electromagnética de un sistema de procesamiento de datos, será castigado con una pena privativa de libertad de hasta dos años o con pena de multa, si el hecho no está conminado en otro precepto con una pena más grave». Además el delito de "Computersabotage" comprendido en el § 303b en la sección sobre los daños materiales, criminaliza la intromisión relevante «en un procesamiento de datos que es de significado esencial para un tercero, de modo que 1) comete el hecho tipificado en el § 303a; 2) introduce o transmite datos (en el sentido del § 202a) con la intención de causar un perjuicio a otro; o 3) destroce, dañe, destruye, inutilice, elimine o modifique un sistema de procesamiento de datos o un soporte de datos», con una pena privativa de libertad de hasta tres años o con pena de multa[71]. En el Código penal italiano se castigan dos ataques contra los sistemas de información. Por un lado, en el Título XII relativo a los "Delitos contra las personas", en el art. 615 ter se considera un "delito contra la inviolabilidad del domicilio" acceder sin autorización a datos y programas informáticos contenidos en todo o en parte de un sistema informático, o mantenerse en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo, castigado con una una pena de prisión de uno a cinco años «si el hecho conduce a la destrucción o daño del sistema o a la interrupción total o parcial de su funcionamiento, o a la destrucción o daño a los datos, información o programas contenidos en el mismo…». Por otro lado, en el Título XIII centrado en los "Delitos contra el patrimonio" se castiga en el art. 635 quater a quien «mediante las conductas mencionadas en el artículo 635 bis», esto es, «destruyendo, deteriorando, borrando, alterando suprimiendo informaciones, datos o programas informáticos ajenos», «o a quien a través de la introducción o transmisión de datos, informaciones o programas informáticos», destruya, dañe o inutilice en todo o en parte un sistema informático o telemático ajeno, u obstaculice de manera grave su funcionamiento.

En sentido similar, se han criminalizado en España determinados ataques contra los sistemas de información dentro del Título X del Código penal sobre los "*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*". En concreto se castiga con una pena de prisión de seis meses a dos años en el art. 197 bis 1 del Código penal 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. En el art. 197 bis 2 del mismo texto legal 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, figura delictiva recogida. Asimismo, en el art. 264 bis del Código penal, dentro del Título XIII acerca de los "*Delitos contra el patrimonio y contra el orden socioeconómico"*, se criminaliza la obstaculización o la interrupción del funcionamiento de un sistema informático ajeno de una manera grave, mediante tres conductas típicas diferentes alternativas: 1) por medio del borrado, daño, deterioro, alteración, supresión o haciendo inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos; 2) a través de la introducción o transmisión de datos; y 3) por la destrucción, el daño, la inutilización, la eliminación o la sustitución del sistema informático, telemático o de almacenamiento de información electrónica.

70 Véase, con carácter general, sobre la tipificación de conductas delictivas en conexión con sistemas informáticos, Romeo Casabona, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», pp. 180 y 181.

71 Véase supra nota 29. El "procesamiento de datos" al que alude este precepto coincide materialmente con la definición de un sistema de información prevista la Directiva 2013/40/UE y en el Convenio del Consejo de Europa sobre Cribercriminalidad. El procesamiento de datos abarca la generalidad de procedimientos matemáticos electrónicos incluyendo su entrada, tratamiento y transferencia en redes internas o externas, pero no comprende procedimientos que no se efectúan de manera electrónica. Véanse Fischer, *Strafgesetzbuch mit Nebengesetzen Kommentar*, 67 Auflage, § 303b, Rn. 5; Hoyer, «§ 303b», SK-StGB, Rn. 5.

Esta técnica de establecer tipos específicos o «tipos de equivalencia» no está exenta de algunos problemas, ya que, por ejemplo, si se vincula un acceso ilícito a un sistema informático del art. 197 bis del Código penal con la protección penal de la intimidad personal y familiar, ¿se puede castigar por este tipo delictivo 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? Las respuestas tienen que ser negativas si se realiza una interpretación teleológico-sistemática del art. 197 bis[72]. Tampoco se le podría castigar al *hacker* por las conductas tipificadas en los arts. 264 y 264 bis del Código penal si no actúa con la intención de producir un borrado, daño, deterioro, alteración, supresión de tal información configurada como dato informático, programa informático o documento electrónico ajeno o con la intención de hacerlos inaccesibles; o si no actúa con la intención de obstaculizar o interrumpir, de manera grave, un sistema informático ajeno mediante conductas que suponen un atentado o una intromisión lesiva en la información contenida en los sistemas de información, mediante la introducción o transmisión de datos; o a través de la destrucción, daño, inutilización, eliminación o sustitución de un sistema informático, telemático o de almacenamiento de información electrónica. Si se opta por esta forma de tipificar los ataques contra los sistemas de información debería preverse también, por ejemplo, el ataque contra un sistema de información que contenga datos reservados de personas jurídicas (art. 200 del Código penal), información sobre la propiedad intelectual (arts. 270 y ss. del Código penal), secretos de empresa (art. 278 del Código penal) o secretos e informaciones relativas a la defensa nacional (art. 598 del Código penal). La elección de incorporar tipos específicos o «tipos de equivalencia» plantea inconvenientes como el excesivo casuismo que conllevaría y la falta de adaptación a la rapidez de los avances tecnológicos que no se previeran en un determinado momento y que impediría aplicar este delito consistente en acceder de manera ilícita a sistemas informáticos a nuevos ámbitos[73].

Al mismo tiempo decantarse por esta opción exige resolver un interrogante: ¿es necesario vincular un tipo penal que castigue un ataque contra los sistemas de información a la protección penal de determinados bienes jurídicos como la intimidad personal y familiar, el patrimonio, etc., para legitimar la intervención del Derecho penal? Tal y como se ha expuesto en el estudio del bien jurídico protegido, es legítima la intervención del Derecho penal en este ámbito por la función que desempeña el bien jurídico protegido en las conductas delictivas contempladas en los arts. 197 bis y 264 bis del Código penal. Recordemos de forma sintética los argumentos: el bien jurídico relativo a la confidencialidad, la integridad y la disponibilidad de los sistemas de información constituye una barrera de contención de riesgos para otros bienes jurídicos que se puedan encontrar involucrados en la función social que desempeñen los sistemas y redes informáticos: la intimidad personal y familiar, el patrimonio, etc. Además, cumple una función positiva de creación y configuración de espacios que delimitan las condiciones en que los bienes jurídicos a los que complementan puedan cumplir realmente su función social, de modo que en estos escenarios enmarcados en la utilización de las TIC se involucran bienes jurídicos tales como el patrimonio,

72 La Circular 3/2017 de la Fiscalía General del Estado, pp. 21 y 22 afirma que «en la práctica será frecuente la concurrencia de este tipo, acceso ilegal a sistemas, con cualquiera de las conductas previstas en el artículo 197 nºs. 1 y 2, particularmente en los supuestos del párrafo segundo consistentes en el acceso a datos registrados en ficheros o soportes informáticos, electrónicos o telemáticos, pues habitualmente estos registros se encuentran protegidos para el acceso directo por medidas de seguridad. En estos casos, la solución habrá de venir por la apreciación, en términos generales, de un concurso medial del artículo 77 del Código penal, como igualmente se produciría en el caso, por ejemplo, de que acceso ilegal tuviera por objeto el descubrimiento de secretos de empresa (art 278 del Código penal) o el descubrimiento de secretos oficiales (art. 598 y ss del Código penal). La razón de ello hay que buscarla en la circunstancia de que el acceso ilegal a un sistema informático afecta a bienes jurídicos no exactamente coincidentes con los que son objeto de protección en los otros tipos penales, no siendo además un medio necesario para la ejecución de los delitos previstos en los artículos 197, 1º y 2º; 278 y 598 y ss. del Código penal. Ello no obsta a que, en supuestos concretos, en los que no sea posible el acceso a la información íntima o a los datos personales por medio distinto a la vulneración de las medidas de seguridad del sistema, pudiera considerarse la posibilidad de apreciar una progresión delictiva que llevaría a considerar el concurso de normas sancionable por la vía del artículo 8.3 del Código penal». Por el contrario y en contra de la FGE al introducirse como delito el acceso ilegal sin autorización a un sistema informático dentro del Título X del CP sobre los "Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio", el legislador lo 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 intimidad personal y familiar que abarca la vida privada de una persona en la que confluyen numerosos derechos vinculados a la propia personalidad.

73 Véanse Romeo Casabona, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», p. 181 y sobre la posible intervención del Derecho penal en la red, con carácter general, Álvarez Vizcaya, «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red», pp. 268 y ss.

la intimidad personal y familiar o la capacidad competitiva de la empresa, de manera que los sistemas de información permiten su desarrollo en las modernas sociedades. La relevancia que tiene este bien jurídico exige más bien la criminalización de aquellas conductas que lo lesionen o lo pongan en peligro a través del establecimiento de nuevos tipos penales genéricos que tipifiquen como delito determinados ataques contra los sistemas de información. Esta opción parece que resulta más idónea al adaptarse a las nuevas formas de criminalidad que pudieran surgir en el futuro, si bien es cierto que implica buscar y encontrar un adecuado lugar sistemático en nuestro Código penal.

Algunos Códigos penales europeos recogen este modelo de tipificación de estas conductas. Así, en el Código penal belga se contemplan diversos ataques contra los sistemas de información en el Título IX bis con la rúbrica "Infracciones contra la confidencialidad, la integridad de los sistemas informáticos y los datos que son almacenados, procesados o transmitidos por estos sistemas". En el art. 550 bis se dispone que «§ 1. El que, sabiendo que no está autorizado para hacerlo, acceda a o se mantenga en un sistema informático, será castigado con prisión de seis meses a dos años y una multa de veintiséis a veinticinco mil euros o solo con una de ellas. Si el delito mencionado en el párrafo 1 se comete con intención fraudulenta, la pena de prisión será de seis meses a tres años. § 2. El que, con intención fraudulenta o de dañar, excede su poder de acceso a un sistema informático, será castigado con prisión de seis meses a tres años y una multa de veintiséis a veinticinco mil euros o solo con una de ellas. § 3. El que se encuentre en una de las situaciones mencionadas en los §§ 1 y 2 y quién 1) tome, de cualquier manera, los datos almacenados, procesados o transmitidos por el sistema informático; 2) haga uso de un sistema informático que pertenece a un tercero o utiliza el sistema informático para acceder al sistema informático de un tercero; 3) causa cualquier daño, incluso sin querer, al sistema informático o a los datos almacenados procesados o transmitidos por ese sistema o al sistema informático de un tercero o los datos almacenados, procesados o transmitidos por ese sistema; será castigado con prisión de uno a cinco años y una multa de veintiséis a cincuenta mil o con una de estas penas solamente…». En el art. 550 ter se prevé «§ 1. El que se ha introducido en un sistema informático, sabiendo que no está autorizado, directa o indirectamente, y modifica o borra datos, o modifica por cualquier medio tecnológico el uso normal de datos en un sistema informático, será castigado con prisión de seis meses a tres años y una multa de veintiséis a veinticinco mil euros o solo con una de estas sanciones. Si el delito mencionado en el párrafo 1 se comete con intención fraudulenta o con el fin de causar daño, la pena de prisión será de seis meses a cinco años. La misma sanción se aplicará cuando el delito mencionado en el párrafo 1 se cometa contra un sistema informático de una infraestructura crítica a que se refiere el artículo 3, 4° de la Ley de seguridad del 1 de julio de 2011 de Protección de infraestructuras críticas. § 2. El que, después de la comisión de un delito mencionado en el § 1, causa daños a los datos en el sistema informático en cuestión o en cualquier otro sistema informático, será castigado con prisión de seis meses a cinco años y una multa de veintiséis a setenta y cinco mil euros o solo con una de esas sanciones. § 3. El que, tras la comisión de un delito mencionado en el § 1, impida total o parcialmente el correcto funcionamiento del sistema informático en cuestión o de cualquier otro sistema informático, será castigado con una pena de prisión de uno a cinco años y una multa de veintiséis a cien mil euros o solo con una de estas sanciones». De una manera muy parecida opera el Código penal francés, en cuyo Libro III, Título II y Capítulo III se recoge un amplio conjunto de atentados contra los sistemas de tratamiento automatizado de datos muy similar al del Código penal belga. También conviene señalar que esta opción de introducir nuevos tipos penales genéricos que tipifiquen como delito determinados ataques contra los sistemas de información, se puede llevar a cabo a través de leyes penales especiales con disposiciones penales materiales, relativas a cuestiones procesales penales y a la cooperación internacional en material penal, como la Lei n.º 109/2009, de 15 de Septiembre, do Cibercrime de Portugal, o el Computer Misuse Act 1990 del Reino Unido con diversas modificaciones posteriores.

La adopción de esta segunda técnica en el Código penal español desde un punto de vista sistemático supone la introducción de una nueva rúbrica, por ejemplo, sobre los "*Delitos contra los sistemas de información y comunicación*"[74], dentro del Título XIII como una modalidad de los delitos contra el orden socioeconómico.

74 Opción por la que se decantan Romeo Casabona, *Derecho penal, Parte Especial*, p. 271; Almenar Pineda, *El delito de hacking*, p. 159. Entiendo que se muestran de acuerdo De la Mata Barranco, *Derecho penal europeo y legislación española: las reformas del Código penal. Actualizado a la reforma penal 2015*, p. 88 cuando afirma que «la tutela de los sistemas de información no es la de la intimidad o la del patrimonio, por mucho que las conductas que puedan afectar estos intereses se asemejen a las que hagan peligrar las infraestructuras críticas que tiene en cuenta la Directiva. Y de una u otra forma el legislador español debiera ser consciente de ello. No sólo tratando de acomodar redacciones legales, sino entendiendo el objetivo comunitario y, en su caso, abordándolo desde ese entendimiento». Y Quintero Olivares, «Artículo 264, 264 bis y 264 ter», p. 205, al concluir que el legislador podría haber aprovechado las últimas reformas del Código penal operadas sobre los arts. 264 y 264 bis, para ubicarlas «en un capítulo o sección independiente y romper definitivamente con las liga-

De esta forma se contemplaría la protección penal de los sistemas de información y comunicación aglutinando aquellas conductas que lesionan o ponen en peligro el bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas informáticos[75]: 1) 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, delito contemplado en el art. 197 bis 1 del Código penal. 2) 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, figura delictiva recogida en el art. 197 bis 2 del Código penal. 3) La obstaculización o interrupción del funcionamiento de un sistema informático ajeno de una manera grave del art. 264 bis del Código penal, mediante las tres conductas típicas diferentes alternativas contempladas en dicho precepto. 4) Los actos preparatorios para cometer cualquiera de los comportamientos expuestos y tipificados en los arts. 197 ter y 264 ter del Código penal. 5) El uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, y causando a éste un perjuicio económico contemplado en el artículo 256 de nuestro texto punitivo, siempre que reúna las características de los ciberataques puros: el objeto y el medio comisivo del ataque son las TIC y sus efectos tienen lugar en el ciberespacio.

V. EL TIPO BÁSICO DEL DELITO DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN

En el art. 264 bis 1 del Código penal se contempla el tipo básico del delito de obstaculización o interrupción del funcionamiento de un sistema de información ajeno mediante tres conductas típicas diferentes alternativas, por lo que estamos ante un **tipo mixto alternativo**[76]. En primer lugar, por medio del borrado, daño, deterioro, alteración, supresión o haciendo inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, que implica, en consecuencia, la realización del delito denominado como "sabotaje informático" del art. 264.1 del Código penal. Esta primera modalidad se encontraba recogida en el anterior art. 264.2 del Código penal: «2. El que por cualquier medio, sin estar autorizado y de manera grave obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, cuando el resultado producido fuera grave, será castigado, con la pena de prisión de seis meses a tres años». En segundo lugar, a través de la introducción o transmisión de datos. Esta manera de obstaculización o interrupción del funcionamiento de un sistema de información ajeno se centra en la afectación del *software* de un sistema de información, mediante la introducción de datos en un sistema de información o la transmisión por la web o por un hardware (USB, CD-ROM, etc.) de programas *malware* (como gusanos, virus, etc.), como afirma Salvadori[77]. En tercer lugar, se castiga la obstaculización o interrupción del funcionamiento de un sistema de información de una manera grave por la destrucción, el daño, la inutilización, la eliminación o la sustitución del sistema informático, telemático o de almacenamiento de información electrónica. Las conductas típicas recaen, entonces, sobre los elementos físicos del correspondiente sistema de información: los aparatos que constituyen el sistema informático (*harware*), telemático o de almacenamiento de información electrónica (memorias externas)[78].

A juicio de Miró LLinares se han recogido todas las conductas que pueden afectar el funcionamiento de un sistema de información, pues resulta difícil imaginar una obstaculización o interrupción por procedimientos de lógica informática que no se realice de alguna de las maneras descritas en el art. 264 bis 1 del Código penal[79]. La denegación de servicios de un sistema de información puede llevarse a cabo de múltiples formas con acciones que, a mero título de ejemplo, 1) consumen repentinamente los recursos de los aparatos afectados, como el procesador, la memoria y/o el disco duro, los puertos de configuración de los *routers*,

duras interpretativas que acompañan al delito común de daños y que son de muy difícil encaje» en los comportamientos delictivos englobados en los mencionados preceptos.

75 Véase también en un sentido similar la opinión de Morón Lerma que estimaba que si se introdujera el delito de acceso ilícito a sistemas informáticos, habría que crear un título autónomo que castigue los atentados a los sistemas informáticos, en el que se ubicara éste y otros incidentes relativos a los mismos, como los daños a los datos y a los sistemas; véase Morón Lerma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», p. 107.

76 Concluyen también que nos encontramos ante un tipo mixto alternativo Guérez Tricarico, «Daños», marginal 11683; Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos*, p. 115.

77 Véase Salvadori, «La regulación de los daños informáticos en el Código penal italiano», p. 48.

78 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4713.

79 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4717.

provocando una caída en su rendimiento; 2) generan grandes cantidades de tráfico desde varios equipos para disminuir su rendimiento o bloquearlos dentro de una red informática; 3) transmiten datos "maliciosos" que provocan la caída de un equipo; 4) proporcionan información falsa sobre tablas de enrutamiento que impiden el acceso a ciertas máquinas de la red mediante *routers* "maliciosos"; 5) activan programas que se replican en el sistema de información, consumiendo la memoria y la capacidad del procesador hasta detener por completo al equipo infectado; 6) provocan la sobrecarga del servidor con el envío masivo de mensajes de correo electrónico ("*mail bombing*"); 7) incumplen reglas de un protocolo; etc[80]. Cualquier denegación de servicio de un sistema de información ocasionado del modo descrito, se puede incluir en alguna de las tres conductas típicas diferentes alternativas contempladas en el art. 264 bis 1 del Código penal. Si ha tenido lugar la destrucción, el daño o la inutilización de un sistema de información ajeno, sin implicar con ello una obstaculización o interrupción de manera grave de su funcionamiento, podemos estimar que se ha producido un delito de daños del art. 263 del Código penal.

Sujeto activo puede serlo cualquier persona, ya que el tipo no requiere ninguna condición personal especial de la autoría. Se trata, en consecuencia, de un delito común. Sujeto pasivo es tanto la comunidad o sociedad directamente interesada en que los sistemas de información proporcionen la función para la que han sido dispuestos, como la persona física o jurídica titular del concreto sistema de información afectado, interrumpido u obstaculizado[81].

El objeto material sobre el que recaen los comportamientos típicos es el propio sistema de información que se compone de unos elementos físicos y lógicos. La definición de un sistema de información se define en el art. 2 de la Directiva 2013/40/UE, y en el art. 7 del Reglamento (UE) 2019/796, 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». Asimismo, en el art. 1 del Convenio del Consejo de Europa sobre Cibercriminalidad se establece que «por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa». Como se puede apreciar en estas definiciones la nota característica del sistema de información es el procesamiento de datos a través de un programa informático[82], a la que hay que añadir también, como apunta Carrasco Andrino, «las notas de programabilidad y variabilidad de los resultados en el tratamiento de los datos, esto es, que el aparato electrónico con el software tenga la capacidad de desarrollar múltiples operaciones con los datos (ejecutarlos, codificarlos, descodificarlos, archivarlos, modificarlos, extraerlos, etc.)»[83]. En sentido similar la SAP Palencia Sección 1ª nº. 42/2016, de 14 julio: concluye que «es verdad que el lenguaje informático ofrece muchas versiones, pero parece que todos estaremos de acuerdo en que, cuando hablamos de sistemas informáticos, nos estamos refiriendo a sistemas que permiten almacenar y procesar información, estamos pues hablando de lo que los informáticos denominan hardware (computadoras, impresoras, escáneres, memorias, lectores de código de barras, estructura de una red de computadoras, etc) y software (manuales de uso, sistema operativo, archivos, documentos, aplicaciones, bases de datos, etc.)». Con más precisión apunta la SAP Valladolid Sección 2ª nº. 82/2020, de 8 junio (ECLI:ES:APVA:2020:440), que «dentro del software cabe incluir, ejemplificativamente, el sistema operativo, el firmware (o programa informático que controla los circuitos internos), las aplicaciones, bases de datos o el driver (programa informático que permite al sistema operativo interactuar con sus periféricos), siendo este una pieza esencial del software y particularmente de su sistema operativo, para que funcionen adecuadamente (entre otros) la impresora, escáner, tarjetas gráficas, de sonido o red, la placa base, etc. Cabiendo, incluso, la posibilidad de incluir en ese concepto el elemento "humano", constituido no sólo por el usuario del sistema informático, también por las personas técnicas

80 Véase una exposición técnica de los diversos tipos de ataques de denegación de servicios (DoS) efectuada por Gómez Vieites, *Seguridad en equipos informáticos*, pp. 63 y ss.; pp. 66 y ss. Véase también el Informe de Ciberamenazas y Tendencias en su edición de 2019 CCN-CERT IA-13/19, elaborado por la Capacidad de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional (CCN-CERT), pp. 41 y ss. En el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información se establece una taxonomía de los ciberincidentes desde un punto de vista técnico y se contemplan diversos ataques de denegación del servicio.

81 Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4721 estima, sin embargo, que sujeto pasivo lo será solo el titular del sistema informático afectado, interrumpido u obstaculizado.

82 Véase Carrasco Andrino, *Derecho penal español, Parte Especial (I)*, 2ª ed., p. 786.

83 Véase Carrasco Andrino, *Derecho penal español, Parte Especial (I)*, 2ª ed., p. 787.

que, entre otros cometidos, elaboran las aplicaciones o subsanan sus deficiencias».

El delito de denegación de servicios de un sistema de información es un delito de resultado al requerirse la obstaculización o interrupción del funcionamiento de un sistema informático ajeno de una manera grave[84]. La obstaculización o interrupción del funcionamiento de un sistema de información implica que no preste sus funciones esenciales ya sea con carácter temporal o permanente[85], aunque la funcionalidad de dicho sistema se pueda reparar de una forma rápida. Conviene subrayar que una obstaculización o interrupción permanente será más bien excepcional. En la SAP de Valencia Sección 4ª nº. 447/2011, de 10 junio (ECLI:ES:APV:2011:3331), se indica que el funcionamiento anómalo de un terminal constituye también «una modalidad de inutilización, parcial si se quiere, pero que determina una perdida de sus cualidades originales, que hace necesario someterlo a algún tipo de reparación o revisión que las restablezca». Como se indica en la Circular 3/2017 de la Fiscalía General del Estado «… el Legislador ha considerado notablemente más graves y peligrosas, porque así lo son efectivamente, las acciones dirigidas contra el sistema informático en su conjunto, que provocan su interrupción u obstaculización de forma grave su normal funcionamiento, respecto de aquellas otras que afectan exclusivamente a los datos, programas o documentos electrónicos, aún cuando tengan incidencia, al menos indirecta, en el sistema en que se integran, siempre que no impliquen una pérdida significativa en la funcionalidad del mismo…»[86].

Para interpretar el elemento valorativo previsto, la gravedad de la obstaculización o interrupción del funcionamiento de un sistema informático ajeno, nos podemos remitir a lo dispuesto en el art. 2 del Reglamento (UE) 2019/796, que dispone que «los factores que determinen si un ciberataque tiene un efecto significativo …, incluirán cualesquiera de los siguientes elementos: a) el alcance, la escala, la repercusión o la gravedad de la perturbación ocasionada; incluido en las actividades económicas y sociales, los servicios esenciales, las funciones fundamentales del Estado, el orden público o la seguridad pública; b) el número de personas físicas o jurídicas, entidades u organismos afectados; c) el número de Estados miembros afectados; d) el importe de las pérdidas económicas ocasionadas, por ejemplo mediante un robo a gran escala de fondos, de recursos económicos o de propiedad intelectual; e) los beneficios económicos obtenidos por el infractor, para sí o para otros; f) la cantidad o la naturaleza de los datos sustraídos o la magnitud de las violaciones de datos; o g) la naturaleza de los datos comercialmente sensibles a los que se haya tenido acceso». La exigencia de una obstaculización o interrupción del funcionamiento de un sistema informático ajeno "grave", permite circunscribir la intervención penal a aquellos supuestos que revistan determinadas características en la valoración de los efectos de dicha obstaculización o interrupción, en la que no deben incluirse solo consideraciones de índole económica o patrimonial, sino también cómo ha incidido la situación en la propia libertad de los titulares de los sistemas de información entre los que se encuentran los Estados, o en la libertad de los usuarios de acceder a los servicios ofrecidos por los sistemas de información[87]. Por ejemplo, en la aludida SAP de Valencia Sección 4ª nº. 447/2011, de 10 junio (ECLI:ES:APV:2011:3331), se valoró como grave la inutilización parcial del sistema operativo de una red de telefonía como consecuencia de la difusión de diversos virus por parte de un individuo, que obligó a su titular a arbitrar un sistema de información para sus clientes, y a dedicar personal especializado para depurar los diferentes terminales afectados, aunque los virus no llegaron a saturar, por su propio efecto contagio, a todo el sistema de mensajería. Por otra parte, en la SAP Palencia Sección 1ª nº. 42/2016, de 14 julio, también calificó de grave la sustitución intencionada de varias tarjetas de memoria con archivos informáticos que eran necesarios para poder proyectar una exposición en una ciudad, por otras tarjetas de memoria «que no funcionaban correctamente ni servían para la finalidad para la que habían sido instaladas, con lo que la finalidad perseguida, es decir, la interrupción de la exposición se consiguió con creces pues la Fundación se vio obligada, por esos hechos, a interrumpirla no por unos días o semanas sino por varios meses… Las consecuencias económicas y los perjuicios para la fundación que, por la exclusiva e intencionada actuación de los acusados, se vio impedida de la correcta utilización del sistema informático empleado para las proyecciones de la exposición, no se derivan de meras posibilidades de inseguros resultados, sino que son fácilmente entendibles a la vista de las circunstancias concurrentes y de las

84 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4717, la Circular 3/2017 de la Fiscalía General del Estado, p. 29, y la SAP Valladolid Sección 2ª nº. 82/2020, de 8 junio (ECLI:ES:APVA:2020:440).

85 Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4717 se refiere solo a la temporalidad de la obstaculización o interrupción.

86 Véase, la Circular 3/2017 de la Fiscalía General del Estado, p. 30.

87 Véase Miró LLinares, «Cibercrímenes económicos y patrimoniales», marginal 4719. De forma menos explícita en la regulación alemana véanse Hoyer, «§ 303b», SK-StGB, Rn. 7; Fischer, *Strafgesetzbuch mit Nebengesetzen Kommentar*, 67 Auflage, § 303b, Rn. 10.

personas que, necesaria y lógicamente, se debieron ver imposibilitadas de presenciar la exposición durante tanto tiempo… En este caso, no estamos pues hablando, como parecen sostener los apelantes, de una simple película donde se veían y oían motivos relativos al Camino de Santiago, si no que la información estaba en formato informático. Es decir, que el material de video y audio instalado estaba en formato digital y para poder procesar esta información era necesario la intervención de un sistema informático, o sea la intervención de las tarjetas que contenían los archivos (hardware) y de aplicaciones específicas para poder procesarlos (software), circunstancias que definen un sistema informático».

Si los hechos perjudican de forma relevante la actividad normal de una empresa, negocio o de una Administración pública, se dispone en el último párrafo del art. 264 bis 1 del Código penal una agravación de la pena. El fundamento de esta agravación se explica por la incidencia graduable que tiene la lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información, en el desarrollo de las funciones que ofrecen a los usuarios la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte o las empresas. Sí que hay que destacar la falta de elementos objetivos que permitan definir el "perjuicio relevante" en la actividad normal de una empresa, negocio o de una Administración pública, lo que puede generar una inseguridad al depender del criterio del juzgador.

El delito de denegación de servicios de un sistema de información de manera grave tipificado en el art. 264 bis 1 del Código penal requiere también la intervención de un autor que actúe "sin estar autorizado", por lo tanto, carece de la disponibilidad sobre el sistema de información o comunicación. Con ello se alude al consentimiento del titular del sistema de información que constituye una causa de exclusión del tipo. En el art. 2 de la Directiva 2013/40/UE se definen los términos «sin autorización» como aquel «*comportamiento al que se refiere la presente Directiva, incluido el acceso, la interferencia o la interceptación, que no haya sido autorizado por el propietario u otro titular del derecho sobre el sistema o parte del mismo o no permitido por el Derecho nacional*». En cuanto al tipo subjetivo del delito del art. 264 bis 1 del Código penal no exige ningún elemento subjetivo de lo injusto adicional distinto del dolo[88].

Por último, debemos reflexionar, por una parte, sobre la relación entre el delito de acceso ilícito a un sistema de información que contiene información personal y familiar, o de mantenerse en el mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo contemplado en el art. 197 bis 1 del Código penal, y el delito de obstaculización o interrupción de manera grave de un sistema informático ajeno mediante las conductas indicadas en el art. 264 bis 1. Como el bien jurídico protegido es el mismo, existe un concurso de leyes entre ambos delitos que se resuelve según el principio de consunción a favor del art. 264 bis 1, puesto que el acceso ilícito a un sistema de información constituye un acto previo normalmente necesario a cualquier obstaculización o interrupción del funcionamiento del sistema, siempre que no concurra alguna autorización. Por otra parte, respecto de la relación entre el delito de daños informáticos del art. 264 del Código penal y el delito de obstaculización o interrupción de manera grave de un sistema informático ajeno mediante las conductas indicadas en el art. 264 bis 1, hay un concurso ideal de delito porque los bienes jurídicos lesionados son distintos: el patrimonio y la confidencialidad, integridad y disponibilidad de los sistemas de información respectivamente.

VI. AGRAVACIONES ESPECÍFICAS

En este epígrafe se van a exponer un conjunto de circunstancias agravantes específicas contempladas en el art. 264 bis 2 y 3 del Código penal. El apartado 2 del mencionado precepto dispone que «se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio causado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior». Estas circunstancias previstas en el art. 264.2 del Código penal son las siguientes: que el hecho «1.ª Se hubiese cometido en el marco de una organización criminal. 2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos. 3.ª El hecho hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad. 4.ª Los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará 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. 5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter. Si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado». Por otra parte, en el art. 264 bis 3

88 Véase Andrés Domínguez, «Artículo 264 bis», p. 360.

se establece que «las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero». A continuación, se analiza el fundamento de estas agravaciones.

1) La obstaculización o interrupción del funcionamiento de un sistema informático ajeno de una manera grave en el marco de una organización criminal

La primera agravación específica se refiere a que el hecho «se hubiese cometido en el marco de una organización criminal», según el art. 264.2 del Código penal. En el art. 9 de la Directiva 2013/40/UE se contempla entre otras circunstancias agravantes que las infracciones relacionadas con la interferencia ilegal en los sistemas de información y en los datos, se castiguen con una sanción máxima de privación de libertad de al menos cinco años cuando: «*a) se cometan en el contexto de una organización delictiva con arreglo a la Decisión marco 2008/841/JAI, con independencia del nivel de la sanción que se establezca en la misma*». El primer interrogante que debe aclararse es qué debemos entender por una organización criminal. El concepto de organización criminal se define normativamente en el art. 570 bis del Código penal como «*la agrupación formada por más de dos personas con carácter estable o por tiempo indefinido, que de manera concertada y coordinada se repartan diversas tareas o funciones con el fin de cometer delitos*». La presencia de un determinado número de personas nos permite hablar de una agrupación: como mínimo tres personas. Por otra parte, esta agrupación de personas debe tener cierta vocación de permanencia (estable o por tiempo indefinido), y se caracteriza por que sus integrantes deben concertarse para la comisión de delitos, lo cual presupone una *organización* en la que es preciso que sus componentes actúen en interés de la agrupación. De ahí se deriva que los hechos delictivos individuales radiquen en el ámbito de actividad de la agrupación definida por sus fines[89]. El fundamento de la agravación que estamos estudiando reside en el efecto criminógeno que tiene una agrupación organizada al configurarse como una situación favorecedora o preparatoria de la comisión de delitos[90]. Múltiples investigaciones han puesto de manifiesto que las organizaciones criminales «se han aprovechado de las TIC para facilitar o mejorar la comisión de delitos, para identificar nuevas oportunidades o para luchar contra las medidas policiales de los Estados destinadas a evitar sus actividades»[91]. La organización criminal aporta un desvalor de lo injusto adicional porque la conducta es más peligrosa (efecto criminógeno actual)[92].

No se ha incorporado en esta agravación, sin embargo, el concepto de grupo criminal recogido en el art. 570 ter del Código penal: «*la unión de más de dos personas que, sin reunir alguna o algunas de las características de la organización criminal definida en el artículo anterior, tenga por finalidad o por objeto la perpetración concertada de delitos*». En los grupos criminales puede faltar o bien la estabilidad o el carácter indefinido de la concertación y coordinación con el fin de cometer delitos, o bien la complejidad organizativa[93]. Llama la atención que no se haya previsto esta agravación fundamentada en la actuación de un grupo criminal para cometer este ciberdelito, porque la naturaleza y las posibilidades que ofrece el ciberespacio favorece más la formación de grupos que no son estables, no tienen un carácter indefinido en la concertación y coordinación para delinquir, o carecen de complejidad organizativa[94]: los miembros de las ciberbandas criminales «no tienen entre sí ningún tipo de contacto físico directo sino que sólo se conocen a través de Internet, en ocasiones desconociendo incluso la identidad real del sujeto y teniendo como única referencia algún tipo de pseudónimo, nick o nombre clave. Al fin y al cabo, esto es perfectamente coherente con la naturaleza y posibilidades que ofrece el ciberespacio: la conjunción de personas situadas en lugares distantes entre sí, pero

89 Véase un estudio más amplio del concepto de organización criminal en Escuchuri Aisa, *Derecho penal, Parte Especial*, pp. 818 y ss.

90 Véase Miró LLinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* pp. 238 y ss.

91 Véanse Miró LLinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* p. 240; Quintero Olivares, «Artículo 264, 264 bis y 264 ter», pp. 201 y 202.

92 Quintero Olivares, «Artículo 264, 264 bis y 264 ter», p. 205, expone que podríamos subsumir en esta agravación la acción ejecutada por sujetos concretos contratados por una organización "no criminal" como, por ejemplo, una empresa que decide dañar a la competencia, aunque ello supondría forzar el concepto de "organización criminal". En mi opinión, en tal supuesto no concurre el fundamento de la agravación que se ha señalado, porque una empresa que opera en el tráfico económico con arreglo a las formalidades legales exigidas, no actúa de manera concertada y coordinada repartiéndose diversas tareas o funciones con el fin de cometer delitos. La misma conclusión cabe alcanzar cuando nos encontremos con Estados que contraten a sujetos concretos para llevar estos comportamientos delictivos. Ni las empresas ni los Estados llevan a cabo materialmente conductas delictivas, que quedan encomendadas a personas físicas.

93 Véase un estudio más amplio del concepto de grupo criminal en Escuchuri Aisa, *Derecho penal, Parte Especial*, pp. 820 y ss.

94 Véase Miró LLinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* p. 240.

unidas por ideas afines y/o por idénticos propósitos, para lo cual colaboran por medio de una estructura de organización de trabajo conjunto»[95]. En todo caso, si nos encontramos con un autor que comete un ataque de denegación de servicios de un sistema de información y comunicación, integrado en un grupo criminal habrá que apreciar un concurso real entre el delito tipificado en el artículo 264 bis y en el artículo 570 ter del Código penal[96].

2) Daños de especial gravedad, afectación a un elevado número de sistemas informáticos o un perjuicio grave al funcionamiento de servicios públicos esenciales o a la provisión de bienes de primera necesidad

Las circunstancias 2.ª y 3.ª del art. 264.2 del Código penal se refieren a que el hecho «haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos», o que «hubiera perjudicado gravemente el funcionamiento de servicios públicos esenciales o la provisión de bienes de primera necesidad». Como ha puesto de manifiesto la Circular 3/2017 de la Fiscalía General del Estado de España el parámetro "gravedad" se reitera de tal modo en la acción y en el resultado de estos comportamientos delictivos, que la determinación de los criterios en orden a una adecuada valoración de este calificativo presenta cierta dificultad[97]. No obstante, se han recogido de manera precursora algunos factores que resuelven si un ciberataque tiene un efecto significativo establecidos en el art. 2 del Reglamento (UE) 2019/796. En la cuantificación de la "especial gravedad" de los daños, de la afectación a un elevado número de sistemas informáticos o del "perjuicio grave" en el funcionamiento de servicios públicos esenciales o a la provisión de bienes de primera necesidad, no se incluyen solo consideraciones de índole económica o patrimonial, sino también cómo ha repercutido el hecho en la propia libertad de los titulares de los sistemas de información entre los que se encuentran los Estados, empresas o particulares, o en la libertad de los usuarios de acceder a los servicios ofrecidos por los sistemas de información[98].

En cuanto a la determinación de los servicios públicos esenciales y los bienes de primera necesidad, debemos remitirnos a lo dispuesto en el art. 2 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y en el art. 3 del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que definen el servicio esencial como aquel que es «necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas». Los sectores estratégicos que dispensan servicios públicos esenciales o bienes de primera necesidad previstos en la Ley 8/2011, de 28 de abril, son la Administración, el espacio, la industria nuclear la industria química, las instalaciones de investigación el agua, la energía, la salud, las TIC, el transporte, la alimentación y el sistema financiero y tributario. El fundamento de estas agravaciones se encuentra en un mayor desvalor del resultado dada la incidencia graduable que tiene la lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información, en el desarrollo de las funciones que ofrecen a los usuarios la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, etc. y el resto de los sectores estratégicos indicados anteriormente.

3) Afectación al sistema de información de una infraestructura crítica o creación de un peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado miembro de la Unión Europea

La circunstancia agravante 4.ª del art. 264.2 del Código penal se centra en que «los hechos hayan afectado al sistema informático de una infraestructura crítica o se hubiera creado una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea. A estos efectos se considerará 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». Podemos concluir, entonces, que se identifica el ataque a un sistema de información de una infraestructura crítica con la creación de una situación de peligro grave para la seguridad del Estado[99]. El concepto de infraestructura crítica asumido en nuestro Código penal nos conduce al art. 2 de la Ley 8/2011, de 28 de abril, y serán aquellas necesarias para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado

95 Véase Miró LLinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* p. 243.
96 Véase, la Circular 3/2017 de la Fiscalía General del Estado, p. 22.
97 Véase, la Circular 3/2017 de la Fiscalía General del Estado, p. 22.
98 Véase *supra*.
99 Véase Barrio Andrés, *Delitos 2.0.*, p. 337.

y las Administraciones Públicas. Asimismo, la definición en dicho precepto de lo que es una infraestructura crítica europea como aquella situada en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección, permite identificar comportamientos que crean una situación de peligro grave para la seguridad de la Unión Europea o de un Estado Miembro de la Unión Europea.

Finalmente, en el aludido art. 2 de la Ley 8/2011 se encuentran recogidos los parámetros en función de los cuales se determina la criticidad y la gravedad de la perturbación o destrucción de una infraestructura crítica en función de: 1) el número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública; 2) el impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios; 3) el impacto medioambiental, degradación en el lugar y sus alrededores; 4) el impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

El fundamento de esta agravación se encuentra también en un mayor desvalor del resultado dada la incidencia que tiene la lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información, en el desarrollo de las diversas funciones sanitarias, económicas, energéticas, etc. que garantizan las infraestructuras críticas, la seguridad del Estado, de la Unión Europea o de un Estado miembro de la Unión Europea. En relación con estos ataques al sistema informático de una infraestructura crítica o que suponen la creación de una situación de peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado Miembro de la Unión Europea, debe tenerse en cuenta que pueden estar dirigidos por Estados (y los grupos patrocinados por estos Estados) contra otros países, sus instituciones, empresas y ciudadanos, lo que constituye una ciberamenaza muy significativa, según el Informe de Ciberamenazas y Tendencias en su edición de 2020 CCN-CERT IA-13/20[100]. La represión penal contra este tipo de agentes requiere una profunda reflexión, y la adopción de instrumentos internacionales adecuados para poder exigir responsabilidades con validez entre los Estados[101].

4) Comisión del hecho por la utilización de determinados instrumentos

La 5.ª circunstancia agravante del art. 264. del Código penal se refiere a que «el delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter», esto es, a) un programa informático, concebido o adaptado principalmente para cometerlo; 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. La utilización de estos medios aporta también un desvalor de lo injusto adicional al delito cometido porque la conducta realizada por los medios indicados es más peligrosa, puesto que evidencia una situación objetiva de peligro que puede facilitar la lesión del bien jurídico.

5) Hechos de extrema gravedad

Por último, en el art. 264.2 *in fine* del Código penal se recoge asimismo una última agravación que «si los hechos hubieran resultado de extrema gravedad, podrá imponerse la pena superior en grado». El fundamento de esta agravación se encuentra en un mayor desvalor del resultado determinado por la incidencia que pueda tener en el caso concreto la lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información, en relación con las funcionalidades que proporcionan tales sistemas en muy diferentes ámbitos.

6) La obstaculización o interrupción de un sistema informático ajeno de una manera grave 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

La obstaculización o interrupción de una manera grave de un sistema informático ajeno mediante la utilización ilícita de datos personales de alguien, para facilitarse el acceso a un sistema de información o para ganarse la confianza de un tercero supone una agravación específica contenida en el art. 264 bis 3 del Código pe-

100 Véase el Informe de Ciberamenazas y Tendencias en su edición de 2020 CCN-CERT IA-13/20, elaborado por la Capacidad de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional (CCN-CERT), p. 12.

101 Véase, con carácter general, Goel, S., «National Cyber Security Strategy and the Emergence of Strong Digital Borders», pp. 82 y 83.

nal[102]. Desde mi punto de vista, esta agravación engloba tres tipos de supuestos. En primer lugar, aquellos en los que el sujeto activo dispone de manera lícita de ciertos datos personales de alguien que puede ser el titular del sistema de información o de un tercero. En segundo lugar, aquellos en los que dicho sujeto activo los ha obtenido de manera ilícita; o, en tercer lugar, aquellos en los que, *ab initio,* el sujeto activo se encuentra con datos de estas características sin haber tomado parte en su descubrimiento o acceso, y en cualquiera de estos casos el sujeto activo los utiliza en la realización de cualquier conducta tipificada en el art. 264 bis 1 del Código penal, para facilitarse el acceso a un sistema de información o para ganarse la confianza de un tercero. El fundamento de esta agravación reside en el efecto criminógeno que tiene disponer de datos personales de una persona, y en la mayor vulnerabilidad de la víctima cuando se utilizan sus datos personales para cometer los delitos tipificados en el art. 264 bis 1 del Código penal.

El objeto material del delito se centra en los "datos personales". Debemos recurrir para su concreción a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y al Reglamento general de protección de datos 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 en cuyo artículo 4.1) se definen los "datos personales" como «*toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*». Por último, debe indicarse que la alusión a la utilización "ilícita" de los datos personales de la víctima hace referencia a la no concurrencia de una causa de justificación.

VII. ACTOS PREPARATORIOS PUNIBLES

En el art. 264 ter del Código penal se penalizan unos actos preparatorios específicos aplicables a los arts. 264 y 264 bis: «*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 dos artículos anteriores: 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*».

La punición de estos actos preparatorios responde a las indicaciones establecidas en el art. 7 de la Directiva 2013/40/UE, en cuyo Considerando nº. 16 se establece que «dadas las diferentes formas en que pueden realizarse los ataques y la rápida evolución de los programas y equipos informáticos, la presente Directiva se refiere a los "instrumentos" que pueden utilizarse para cometer las infracciones enumeradas en la presente Directiva. Dichos instrumentos pueden ser programas informáticos maliciosos, incluidos los que permiten crear redes infectadas, que se utilizan para cometer ciberataques. Aun cuando uno de estos instrumentos sea adecuado o incluso especialmente adecuado para llevar a cabo las infracciones enumeradas en la presente Directiva, es posible que dicho instrumento fuera creado con fines legítimos. Teniendo en cuenta la necesidad de evitar la tipificación penal cuando estos instrumentos sean creados y comercializados con fines legítimos, como probar la fiabilidad de los productos de la tecnología de la información o la seguridad de los sistemas de información, además del requisito de intención general también debe cumplirse el requisito de que dichos instrumentos sean utilizados para cometer una o varias de las infracciones enumeradas en la presente Directiva». La tipificación de estos actos preparatorios en el contexto de las nuevas tecnologías y del ciberespacio, se fundamenta en el peligro que supone su realización para bienes jurídicos individuales y la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, lo que ha significado una adaptación de la regulación penal a dicho contexto. Algunos autores han señalado también que con la tipificación de estas conductas se asegura el castigo, entre otras, de determinadas conductas calificables como tentativa de participación, cuya punición sería cuestionable sin su previsión expresa[103]. Las conductas típicas castigadas

102 La Directiva 2013/40/UE contempla en su art. 9 una agravación aplicable, entre otras, a las conductas de obstaculización o interrupción significativas del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización (art. 4), consistente en castigar con una sanción máxima de privación de libertad de al menos cinco años cuando: «sean cometidas utilizando ilícitamente datos de carácter personal de otra persona con la finalidad de ganar la confianza de un tercero, causando así daños al propietario legítimo de la identidad …, a menos que tal circunstancia ya esté contemplada en otra infracción que sea sancionable con arreglo al Derecho nacional».

103 En relación con los mismos actos preparatorios recogidos en el art. 197 ter del Código penal, véanse Castiñeira Palou/Estrada i Cuadras, *Lecciones de Derecho penal, Parte Especial,* 4ª ed., p. 166; Anarte Borrallo/Doval País, «Efectos de la reforma de 2015 en los delitos contra la intimidad», p. 1259.

son cuatro: 1) producir, 2) adquirir para su uso 3) importar o 4) facilitar a terceros de cualquier modo: 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, a las que se añade un elemento subjetivo de lo injusto, "para facilitar la comisión de alguno de los delitos tipificados en los arts. 264 y 264 bis del Código penal".

Por último, debemos señalar que no se plantea ningún solapamiento entre las conductas tipificadas en el art. 197 ter y las del art. 264 ter del Código penal, puesto que el elemento subjetivo de lo injusto las diferencia claramente: en el art. 197 ter se castiga producir, adquirir para su uso, importar o facilitar a terceros de cualquier modo, «con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1º y 2º 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», mientras que en el art. 264 ter se penalizan idénticos comportamientos con la intención de facilitar la comisión de alguno de los delitos a que se refieren los arts. 264 y 264 bis[104].

VIII. LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS

La Directiva 2013/40/UE contempla en su art. 10 la obligación de que los Estados prevean la responsabilidad de las personas jurídicas: «1. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables de las infracciones mencionadas en los artículos 3 a 8 cuando estas infracciones sean cometidas en su beneficio por cualquier persona que, actuando a título particular o como parte de un órgano de la persona jurídica, ostente un cargo directivo en el seno de dicha persona jurídica, basado en: a) el poder de representación de dicha persona jurídica, o b) la capacidad para tomar decisiones en nombre de dicha persona jurídica, o c) la capacidad para ejercer un control en el seno de dicha persona jurídica. 2. Los Estados miembros adoptarán las medidas necesarias para garantizar que las personas jurídicas puedan ser consideradas responsables cuando la falta de supervisión o control por parte de alguna de las personas a que se refiere el apartado 1º haya permitido que una persona sometida a su autoridad cometa una de las infracciones mencionadas en los artículos 3 a 8 en beneficio de esa persona jurídica. 3. La responsabilidad de las personas jurídicas en virtud de los apartados 1º y 2º no excluirá la incoación de acciones penales contra las personas físicas que sean autoras, inductoras o cómplices de las infracciones mencionadas en los artículos 3 a 8». Con la reforma operada por la LO 1/2015, de 30 de marzo, se añadió dicha responsabilidad penal en nuevo art. 264 quáter a los ataques de denegación de servicios con el siguiente tenor literal: «Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los tres artículos anteriores, se le impondrá las siguientes penas: a) Multa de dos a cinco años o del quíntuplo a doce veces el valor del perjuicio causado, si resulta una cantidad superior, cuando se trate de delitos castigados con una pena de prisión de más de tres años. B) Multa de uno a tres años o del triple a ocho veces el valor del perjuicio causado, si resulta una cantidad superior, en el resto de los casos. 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».

Con carácter general, el reconocimiento de responsabilidad penal a las personas jurídicas en el art. 31 bis de nuestro Código penal a partir de la reforma operada por la LO 5/2010, de 22 de junio, ha suscitado una vehemente discusión científica entre partidarios y detractores de tal entidad que, en algunos casos y con toda la razón, ha generado posiciones de auténtica sublevación para defender los postulados de una dogmática penal coherente con sus fundamentos[105]. En este trabajo no nos vamos a centrar en los problemas que plantea el reconocimiento de una pretendida responsabilidad penal de las personas jurídicas, porque excede, con creces, su objetivo. No obstante, en el marco de este "pretendido" reconocimiento de responsabilidad penal a las personas jurídicas, conviene recordar la necesidad de que las personas jurídicas que en sus actividades requieran la

Para nuestra jurisprudencia existe un concurso medial entre las conductas tipificadas en el artículo 264 bis y las del artículo 264 ter. Véase la SAP Valladolid Sección 2ª nº. 82/2020, de 8 junio (ECLI:ES:APVA:2020:440). Sin embargo, como el bien jurídico que lesionan o ponen en peligro es la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación, la relación entre estos preceptos es la de un concurso de leyes a resolver por el criterio de la consunción.

104 Véase Castelló Nicas, «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor», p. 510.

105 Véanse, por ejemplo, las exposiciones de Gracia Martín, «Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la persona jurídica», pp. 1 y ss.; Schünemann, «Die aktuelle Forderung einer Verbandsstrafe –ein kriminalpolitischer Zombie», pp. 1 y ss.; Gómez Martín, «Penas para personas jurídicas: ¿ovejas con piel de lobo?», pp. 247 y ss.

utilización del ciberespacio con sistemas de redes telemáticas, abiertas o cerradas, establezcan los correspondientes «modelos de organización y gestión» a que se refiere la condición 1ª del apartado 2º y del 4º del art. 31 bis del Código penal, con el fin de evitar la comisión del delito recogido en el art. 264 bis del Código penal. Tales modelos se pueden recoger en los "planes directores de ciberseguridad" de las empresas con una organización y gestión del personal, recursos técnicos, legales, de procedimiento interno, de formación de los empleados, etc[106]..

IX. REFLEXIONES EN TORNO A LA DETERMINACIÓN DE LA LEY PENAL APLICABLE EN LOS ATAQUES DE DENEGACIÓN DE SERVICIOS TRANSFRONTERIZOS

Anteriormente, hemos indicado que en los ataques contra los sistemas de información y comunicación podemos encontrar una nota que le añade un especial grado de peligrosidad: su conexión internacional o transfronteriza, de modo que sus actuaciones pueden ir más allá de un ámbito geográfico concreto. Ello implica que, si no existe una armonización de las legislaciones penales en torno a la configuración típica y castigo de estos comportamientos, objetivo previsto a través de diversos instrumentos internacionales, como el Convenio del Consejo de Europa sobre Cibercriminalidad o la Directiva 2013/40/UE, pueden quedar impunes si el lugar donde se ha cometido el correspondiente ataque no lo contempla como infracción penal. No obstante, hay que tener en cuenta lo que indica Flores Mendoza en relación con los ciberdelitos: estas conductas tienen múltiples lugares de comisión por la utilización de Internet[107]. En relación con el delito de denegación de servicios de un sistema de información debemos subrayar que es un delito de resultado. En nuestro ordenamiento jurídico, coincidente con nuestro entorno, el principio de territorialidad es de aplicación preferente y la determinación del lugar o lugares de comisión de un delito se resuelve según la teoría de la ubicuidad sostenida mayoritariamente, de modo que el lugar de comisión del delito es aquel en el que haya tenido lugar total o parcialmente el delito; esto es, bastaría que la acción, una parte de ella o tan solo el resultado tuviese lugar en el territorio sometido a la soberanía de un estado para ejercitar la jurisdicción conforme al principio de territorialidad[108].

X. LA PENALIZACIÓN DE LOS ATAQUES DE DENEGACIÓN DE SERVICIOS COMO CIBERDELITO EN EL CÓDIGO PENAL ESPAÑOL, ¿OFRECE UNA RESPUESTA ADECUADA FRENTE A LAS AMENAZAS Y ATAQUES QUE SE CIERNEN SOBRE LA CIBERSEGURIDAD?

Finalmente, debemos valorar si el incesante desarrollo tecnológico podría desactualizar las conductas delictivas tipificadas en el art. 264 bis 1 del Código penal en un breve espacio de tiempo. Como hemos señalado anteriormente, en dicho precepto se han previsto todas las conductas que pueden afectar el funcionamiento de un sistema de información y de comunicación. No obstante, cabe mejorar el conjunto de agravaciones que giran en torno a la mayor gravedad del desvalor del resultado, ya que la regulación actual resulta muy reiterativa y plantea dificultades interpretativas que producen inseguridad jurídica. Se podría haber incorporado una sola agravación de la pena «cuando el hecho revista especial gravedad atendiendo al perjuicio ocasionado según los intereses generales afectados», con el fin de atender la incidencia graduable que tiene la lesión del bien jurídico relativo a la confidencialidad, integridad y disponibilidad de los sistemas de información, en el desarrollo de las funciones que ofrecen a los usuarios la Administración pública, el sistema financiero, el sistema sanitario, las infraestructuras básicas de transporte, las empresas, etc.

También merece la pena destacar que las posibles deficiencias detectadas en relación con los ataques de denegación de servicios no parecen encontrarse en el ámbito de la regulación jurídico penal nacional, sino más bien en la cooperación jurídica y judicial internacional. El Convenio del Consejo de Europa sobre Cibercriminalidad (Budapest, 23 de noviembre de 2001) constituye hoy en día en una herramienta fundamental para asegurar el Estado de Derecho en el ciberespacio y ha sido ratificado por 46 países miembros del Consejo de Europa y por 22 países que no lo son. Este Convenio se ha completado con el Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos de 28 de enero de 2003, y con el Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas de 12 de abril de 2021. No obstante, la doctrina señala

106 Véase el contenido de un plan director de seguridad elaborado por el INCIBE disponible en el enlace https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

107 Véase Flores Mendoza, «Análisis del lugar de comisión de los ciberdelitos de contenido. ¿Impunidad o universalización del delito?», p. 140.

108 Véase Flores Mendoza, «Análisis del lugar de comisión de los ciberdelitos de contenido. ¿Impunidad o universalización del delito?», p. 134.

que el bajo nivel en la implementación del Convenio por parte de los Estados no está permitiendo obtener todos los beneficios que se derivarían del mismo[109]. Por otra parte, la Unión Europea, Naciones Unidas, la Organización del Tratado del Atlántico Norte junto con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y la Unión Internacional de Telecomunicaciones (UIT), entre otras, proponen también en el ámbito de la cibercriminalidad un tipo de cooperación fundamentalmente de carácter asistencial que fomente la creación de capacidades por parte de los Estados para avanzar en la resiliencia frente a este tipo de delincuencia[110]. El impulso a la cooperación jurídica y judicial internacional así como asistencial entre los Estados debe ayudar a implantar el Estado de Derecho en el ciberespacio, aunque esta tarea requiere mucho tiempo.

XI. BIBLIOGRAFÍA

Almenar Pineda, *El delito de hacking*, Thomson Reuters Aranzadi, Cizur Menor, 2018.

Almenar Pineda, *Ciberdelincuencia*, Porto Editorial Juruá, 2018

Alonso de Escamilla, *Delitos. La parte especial del Derecho penal*, 3ª ed., Lamarca Pérez (Coord.), Colex, Madrid, 2015.

Álvarez Rodríguez, «Constitución y Derecho del Ciberespacio», *Nuevos retos de la ciberseguridad en un contexto cambiante,* Mallada Fernández Dir., Thomson Reuters Aranzadi, Cizur Menor, 2019.

Álvarez Vizcaya, «Consideraciones político criminales sobre la delincuencia informática: el papel del Derecho penal en la red», *Internet y Derecho penal*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2002.

Anarte Borrallo/Doval País, «Efectos de la reforma de 2015 en los delitos contra la intimidad», p. 1259.

Anarte Borrallo/Doval País, *Derecho penal, Parte Especial, Volumen I, La protección penal de los intereses jurídicos personales. (Adaptado a la reforma de 2015 del Código penal)*, Boix Reig (Dir.), 2ª ed., Iustel, Madrid, 2016.

Andrés Domínguez, «Artículo 264 bis», Comentarios Prácticos al Código penal, Delitos contra el patrimonio y socioeconómicos, Artículos 234-318 bis, Tomo III, Gómez Tomillo Dir., Thomson Reuters Aranzadi, Pamplona, 2015.

Barrio Andrés, *Delitos 2.0. Aspectos penales, procesales y de seguridad de los ciberdelitos,* Wolters Kluver, Madrid, 2018.

Barrio Andrés, *Manual de Derecho digital,* Tirant lo Blanch, Valencia, 2020.

Benítez Ortúzar, *Sistema de Derecho penal, Parte Especial,* 2ª ed., Morillas Cueva Dir., Dykinson, Madrid, 2016.

Bolea Bardon, *Comentarios al Código penal. Reforma LO 1/2015 y LO 2/2015,* Corcoy Bidasolo/Mir Puig Dirs., Vera Sánchez Coord., Tirant lo blanch, Valencia, 2015.

Bustos Ramírez, «Del estado actual de la teoría del injusto», *Control social y sistema penal*, PPU, Barcelona, 1987.

Bustos Ramírez, «Los bienes jurídicos colectivos. (Repercusiones de la labor legislativa de Jiménez de Asúa en el Código Penal de 1932)», *Revista de la Facultad de Derecho de la Universidad Complutense*, nº. 11.

Bustos Ramírez, «Perspectivas actuales del Derecho Penal Económico», *Política criminal y reforma penal. Homenaje a la memoria del Profesor Dr. D. Juan del Rosal,* Editorial Revista de Derecho privado, Editoriales de Derecho Reunidas, Madrid, 1993.

Bustos Ramírez, «Política criminal e injusto. (Política criminal, bien jurídico, desvalor de acto y de resultado)», *Control social y sistema penal*, PPU, Barcelona, 1987.

Bustos Ramírez/Hormazábal Malarée, *Lecciones de Derecho penal*, Parte General, Editorial Trotta, Madrid, 2006.

Carrasco Andrino, *Derecho penal español, Parte Especial (I)*, 2ª ed., Álvarez García (Dir.), Manjón-Cabeza/Ventura Püschel (Coords.), Tirant lo blanch, Valencia, 2011.

Castelló Nicas, «Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio, y delitos contra el honor», *Estudios sobre el Código*

109 Véase Segura Serrano, «Ciberseguridad y Derecho internacional», p. 295.

110 Véase Segura Serrano, «Ciberseguridad y Derecho internacional», p. 299. Véase también Goel, S., «National Cyber Security Strategy and the Emergence of Strong Digital Borders», pp. 82 y 83, que señala que la Organización para la Cooperación y el Desarrollo Económicos (OSCE) también ha trabajado en el desarrollo de medidas de fomento de la confianza durante los últimos años, cuyo objetivo es mejorar la transparencia entre los Estados mediante la promoción del intercambio de información y la comunicación entre los responsables de la formulación de políticas y la toma de decisiones en relación con el ciberespacio. Estas medidas no detendrán un conflicto intencionado, pero posiblemente frenen su escalada.

penal reformado. (Leyes Orgánicas 1/2015 y 2/2015), Dykinson, Madrid, 2015.

Castiñeira Palou/Estrada i Cuadras*, Lecciones de Derecho penal, Parte Especial, 4ª ed. adaptada a la LO 1/2015 de reforma del CP,* Silva Sánchez (Dir.), Ragués i Vallès (Coord.), Atelier, Barcelona, 2015.

Cerezo Mir, Curso de Derecho penal español, Parte General, I. Introducción, 6ª ed., Tecnos, Madrid, 2004.

Circular 3/2017 de la Fiscalía General del Estado, 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, disponible en el enlace https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf.

Costas Sanchos, *Seguridad informática*, RA-MA Editorial, Madrid, 2014.

Colás Turégano, «Nuevas conductas delictivas contra la intimidad (arts. 197; 197 bis; 197 ter)», Comentarios a la reforma del Código penal de 2015, González Cussac Dir., Matallín Evangelio/Górriz Royo Coords., Tirant lo blanch, Valencia, 2015.

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

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

De Miguel Beriain, *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, Romeo Casabona/Sola Reche/Boldova Pasamar coords., Comares, Granada, 2016.

Escuchuri Aisa, *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, Romeo Casabona/Sola Reche/Boldova Pasamar coords., Comares, Granada, 2016.

Fernández Bermejo/Martínez Atienza, *Ciberseguridad, ciberespacio y ciberdelincuencia,* Thomson Reuters Aranzadi, Cizur Menor, 2018.

Fischer, «§ 303b», *Strafgesetzbuch mit Nebengesetzen Kommentar*, 67 Auflage, C. H. Beck, 2020.

Flores Mendoza, «Análisis del lugar de comisión de los ciberdelitos de contenido. ¿Impunidad o universalización del delito?», *Cuadernos de Política Criminal*, nº. 128, 2019.

Goel, S., «National Cyber Security Strategy and the Emergence of Strong Digital Borders», *Connections QJ 19*, nº. 1, 2020.

Gómez Martín, «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3º CP). A la vez, un estudio sobre los delitos de emprendimiento o preparación en el CP de 1995», Revista electrónica de ciencia penal y criminología, nº. 4, 2002.

Gómez Martín, «Penas para personas jurídicas: ¿ovejas con piel de lobo?», *Prisión y alternativas en el nuevo Código Penal tras la reforma 2015*, Mirena Landa/Ortubay Fuentes/Garro Carrera coords., Dykinson, Madrid, 2017.

Gómez Vieites, *Seguridad en equipos informáticos,* Starbook, Madrid, 2014.

González Cussac, *Derecho penal, Parte Especial*, 5ª ed. actualizada a la Ley Orgánica 1/2015, González Cussac coord., Tirant lo blanch, Valencia, 2016.

González Rus, «Daños a través de internet y denegación de servicios», *Homenaje al profesor Dr. Gonzalo Rodríguez Mourullo,* Jorge Barreiro y otros coords., Civitas, Madrid, 2005.

González Rus, «Los ilícitos en la red (I): hackers, crakers cyberpunks, sniffers, denegación del servicio y otros comportamientos semejantes», *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Romeo Casabona coord., Comares, Granada, 2006.

González Rus, «Precisiones conceptuales y político-criminales sobre la intervención penal en Internet», *Delito e informática: algunos aspectos,* Cuadernos penales José María Lidón, número 4, 2007, Bilbao, Universidad de Deusto.

Gracia Martín, «El finalismo como método sintético real-normativo para la construcción de la teoría del delito», *Revista Electrónica de Ciencia Penal y Criminología* 06-07 (2004).

Gracia Martín, «Nuevas perspectivas del Derecho penal tributario. (Las "funciones del tributo" como bien jurídico)», *Actualidad Penal,* nº. 10, 1994.

Gracia Martín, Fundamentos de dogmática penal. Una introducción a la concepción finalista de la responsabilidad penal, Atelier, Barcelona, 2006.

Gracia Martín, Prolegómenos para la lucha por la modernización y expansión del Derecho penal y para la crítica del discurso de resistencia, Tirant lo Blanch, Valencia, 2003.

Gracia Martín, «Crítica de las modernas construcciones de una mal llamada responsabilidad penal de la

persona jurídica», *Revista Electrónica de Ciencia Penal y Criminología* 18-05 (2016).

Guérez Tricarico, «Daños», Memento Práctico Penal, Francis Lefebvre, Madrid, 2016.

Gutiérrez Francés, «Delincuencia económica e informática en el nuevo Código penal», *Ámbito jurídico de las tecnologías de la información*, Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 1996.

Gutiérrez Francés, «El intrusismo informático (Hacking): ¿Represión penal autónoma?», *Informática y Derecho, II Congreso Internacional de Informática y Derecho, Actas, Volumen II*, números 12-15, 1996.

Gutiérrez Francés, «Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa», *Estudios de Derecho penal económico,* Tiedemann/Arroyo Zapatero editores, Ediciones de la Universidad de Castilla-La Mancha, 1994.

Gutiérrez Francés, *Fraude informático y estafa*, Madrid, 1991.

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

Hilgendorf/Frank/Valerius, *Computer- und Internetstrafrecht. Ein Grundriss,* Springer, Berlin, 2005.

Himanen, *La ética del hacker y el espíritu de la era de la información,* Prólogo de Linus Torvalds y Epílogo de Manuel Castells, Ediciones Destino, Madrid, 2002.

Hoyer, «§ 303b», *Systematischer Kommentar zum Strafgesetzbuch, Band VI,* § 303-358 StGB, 9 Auflage, Carl Heymanns Verlag, 2016.

Huidobro Moya/Roldán Martínez, *Seguridad en redes y sistemas informáticos,* Thomson Paraninfo, 2005.

Informe de Ciberamenazas y Tendencias en su edición de 2019 CCN-CERT IA-13/19, elaborado por la Capacidad de Respuesta a Incidentes de Seguridad del Centro Criptológico Nacional (CCN-CERT).

Lackner/Kühl, «§ 303b», *Strafgesetzbuch Kommentar*, 29 Auflage, C. H. Beck, 2018.

Lezertúa, «El proyecto de Convenio sobre el cibercrimen del Consejo de Europa», *Internet y Derecho penal, Cuadernos de Derecho Judicial,* López Ortega Dir., Madrid, Consejo General del Poder Judicial, 2001.

Longstaff/Ellis/Hernan/Lipson/McMillan/Pesante/Simmel, «Security of the Internet», *The Froehlich/Kent Encyclopedia of Telecommunications*, Marcel Dekker, New York, 1997, vol. 15.

López Gorostidi, «Los valores tradicionales como bienes jurídicos protegidos también en el ciberespacio: apropósito del confinamiento provocado por la crisis sanitaria del COVID-19», *Revista Penal*, nº 47, 2021.

Lucena Cid, «El concepto de la intimidad en los nuevos contextos tecnológicos», La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación, Galán Muñoz Coord., Tirant lo blanch, Valencia, 2014.

Maiwald, *Fundamentos de seguridad de redes,* 2ª ed., McGraw-Hill Interamericana Editores, México, 2003.

Mansfield, Defensa contra hackers. Protección de información privada, Ediciones Anaya Multimedia, Madrid, 2001.

Mata y Martín, *Delincuencia informática y Derecho penal*, Edisofer, Madrid, 2001.

Matellanes Rodríguez, «Vías para la tipificación del acceso ilegal a los sistemas informáticos (I)», Revista Penal nº 22, 2008.

Matellanes Rodríguez, «Vías para la tipificación del acceso ilegal a los sistemas informáticos (y II)», Revista Penal nº 23, 2009.

Mayo Calderón, *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, Romeo Casabona/Sola Reche/Boldova Pasamar coords., Comares, Granada, 2016.

Mestre Delgado, *Delitos, La parte especial del Derecho penal,* 3ª ed., Lamarca Pérez coord., Colex, Madrid, 2015.

Mir Puig, «Sobre algunas cuestiones relevantes del derecho penal en internet», *Internet y Derecho penal,* Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, Madrid, 2002.

Miró LLinares, «Cibercrímenes económicos y patrimoniales», Memento Práctico Penal Económico y de la Empresa, Francis Lefebvre, Madrid, 2016.

Miró LLinares, «Delitos informáticos. Hacking. Daños», *Memento Experto. Reforma Penal*, Ortiz de Urbina Gimeno (coord.), Ed. Ediciones Francis Lefebvre, 1ª edición, Madrid, 2010.

Miró LLinares, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio,* Marcial Pons, Madrid, Barcelona, Buenos Aires, São Paolo, 2012.

Miró LLinares, «Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y

adaptación situacional de ciberdelitos», Revista de internet, derecho y política, n.º 32, marzo, 2021, pp.

Möhrenschlager, «Das neue Computerstrafrecht», *Wistra* 1986.

Morales García, «Apuntes de política criminal en el contexto tecnológico. Una aproximación a la Convención del Consejo de Europa sobre *Cyber-Crime»,* Delincuencia informática. Problemas de responsabilidad, Cuadernos de derecho judicial, nº. 9, Morales García (Dir.), 2002.

Morales García, «Delincuencia informática: intrusismo, sabotaje informático y uso ilícito de tarjetas (arts. 197.3 y 8, 264 y 248», *La reforma penal de 2010: análisis y comentarios,* Thomson Reuters, 2010.

Morales Prats, *Comentarios a la Parte Especial del Derecho penal*, Quintero Olivares (Dir.), Morales Prats (Coord.), 10ª ed., Aranzadi Thomson Reuters, 2016.

Morón Lerma, «Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos», *Delito e informática: algunos aspectos, Cuadernos penales José María Lidón*, número 4, 2007, Bilbao, Universidad de Deusto.

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

Morón Lerma/Rodríguez Puerta, «Traducción y breve comentario del Convenio sobre Cibercriminalidad», *Revista de derecho y proceso penal*, nº. 7, 2002.

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

Navarro Frías, *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30 de marzo*, Romeo Casabona/Sola Reche/Boldova Pasamar coords., Comares, Granada, 2016.

Nemzov, *Strafbarkeit von Online-Blockaden und DDoS-Angriffen vor und nach dem Inkrafttreten des 41. Strafrechtsänderungsgesetzes unter Berücksichtigung von verfassungsrechtlichen und europarechtlichen Vorgaben*, Verlag Dr. Kovač, Hamburg, 2017.

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

Piqueres Castellote, «Conocimientos básicos en internet y utilización para actividades ilícitas», *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?*, Velasco Núñez (Dir.), Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2006.

Puente Alba, «Propuestas internacionales de criminalizar el acceso ilegal a sistemas informáticos: ¿Debe protegerse de forma autónoma la seguridad informática?», *Nuevos retos del Derecho penal en la era de la globalización,* Faraldo Cabana Dir., Brandariz García/Puente Aba Coords., Tirant lo blanch, Valencia, 2004.

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

Quesada Morales, «La protección penal de los sistemas de información: Normativa actual y perspectivas de futuro», Revista Aranzadi de Derecho y Nuevas Tecnologías, nº. 4, 2004.

Quintero Olivares, «Artículo 264, 264 bis y 264 ter», *Comentarios al Código penal*, Tomo II (Artículo 234 a disposición final 7ª), Quintero Olivares (Dir.), Morales Prats (Coord.), 7ª ed., Aranzadi Thomson Reuters, 2016.

Renobell Santaren, «Hacktivismo digital: de la cultura hacker a los delitos digitales», *Nuevo retos de la ciberseguridad en un contexto cambiante,* Mallada Fernández Dir., Thomson Reuters Aranzadi, 2019,

Ribagorda Garnacho, «Seguridad de las tecnologías de la información», *Ámbito jurídico de las tecnologías de la información,* Consejo General del Poder Judicial, 1996.

Ribagorda Garnacho, «La protección de datos personales y la seguridad de la información», Revista Jurídica de Castilla y León, nº 16, septiembre, 2008.

Rodríguez Bernal, «Los cibercrímenes en el espacio de libertad, seguridad y justicia», Revista Aranzadi de derecho y nuevas tecnologías, nº. 5, 2004.

Rodríguez Mourullo/Alonso Gallo/Lascuraín Sánchez, «Derecho penal e internet», *Régimen jurídico de internet,* Cremades, Fernández-Ordoñez, Illescas coords., Editorial La Ley, Madrid, 2002.

Romeo Casabona, «De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal», *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales,* Comares, Granada, 2006.

Romeo Casabona, «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», Poder Judicial, nº. 31, 1993.

Romeo Casabona, *Derecho penal, Parte Especial conforme a las leyes orgánicas 1 y 2/2015, de 30*

de marzo, Romeo Casabona/Sola Reche/Boldova Pasamar coords., Comares, Granada, 2016.

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

Rueda Martín, La nueva protección de la vida privada y de los sistemas de información en el Código penal, Atelier, Barcelona, 2018.

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

Rueda Martín, Protección penal de la intimidad personal e informática. (Los delitos de descubrimiento y revelación de secretos de los artículos 197 y 198 del Código penal, Atelier, Barcelona, 2004.

Salom Clotet, «Delito informático y su investigación», *Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?,* Velasco Núñez (Dir.), Cuadernos de Derecho Judicial, Consejo General del Poder Judicial, 2006.

Salvadori, «La regulación de los daños informáticos en el Código penal italiano» *Revista de internet, Derecho y política,* nº. 16, junio 2013, p. 48.

Sánchez Bravo, «El Convenio del Consejo de Europa sobre cibercrimen: control vs. Libertades públicas», La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía, nº. 3, 2002.

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

Schulze-Heiming, *Der strafrechtliche Schutz von Computerdaten gegen die Angriffsformen ser Spionage, Sabotage und des Zeitdiebstahls*, Waxmann Verlag, Münster, New York, 1995.

Schünemann, «Die aktuelle Forderung einer Verbandsstrafe –ein kriminalpolitischer Zombie», ZIS 1/2014.

Segura Serrano, «Ciberseguridad y Derecho internacional», *Revista Española de Derecho Internacional*, Vol. 69/2, julio-diciembre 2017.

Sieber, «Documentación para una aproximación al delito informático», *Delincuencia informática,* Mir Puig (coord.), PPU, 1992.

Sieber, «Legal Aspects of Computer-Related Crime in the Information Society —Comcrime-Study—, prepared for the European Commission by Frof. Dr. Ulrich Sieber, versión de enero de 1998.

Sieber, *Computerkriminalität und Strafrecht*, 1ª ed., Heymann, Munich, 1977.

Stytz/Bank, «Cyber Warfare Simulation to Prepare to Control Cyber Space», National Cybersecurity Institute Journal, 2014, vol 1, nº 2.

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

Stree/Hecker, *Schönke/Schröder, Strafgesetzbuch Kommentar*, 30 Auflage, C. H. Beck, 2019.

Terradillos Basoco, «La satisfacción de necesidades como criterio de determinación del objeto de tutela jurídico-penal», *Revista de la Facultad de Derecho de la Universidad Complutense*, nº. 63, 1981.

Tomás y Valiente Lanuza, *Comentarios prácticos al Código penal. Los delitos contra las personas, artículo 138-233,* Gómez Tomillo Dir., Tomo II, 1ª ed., Thomson Reuters, Madrid, 2015.

United Nations Manual on the prevention and control of Computer-Related Crime, *International Review of Criminal Policy,* nº. 43 y 44, 1994, parágrafo 74.

Velasco Núñez, *Delitos tecnológicos. Cuestiones penales y procesales*, Wolters Kluver, Madrid, 2021.

Wolf, «§ 303b», *Strafgesetzbuch. Leipziger Kommentar Großkommentar*, Laufhütte/Rissing-van Saan/ Tiedemann Hrsg., Band 10, 12 Auflage, De Gruyter, Berlin, 2008.

Zaczyk, «§ 303b», *NomosKommentar Strafgesetzbuch*, Kindhäuser/Neumann/Paeffgen Hrsg., Band 3, 5 Auflage, Nomos Verlagsgesellschaft, Baden-Baden, 2017.