Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado

IVAN SALVADORI

Doctor europeo en Derecho Penal Económico y Derecho Penal Informático, becario de investigación de la Universidad de Verona-Universitat de Barcelona

RESUMEN

En el presente trabajo se analiza la formulación y la ubicación de las nuevas normas que protegen la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, que se han introducido en el Código Penal español por la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la LO 10/1995, de 23 de noviembre, del Código Penal. A este respecto se otorgará especial atención a los nuevos delitos de acceso ilícito a datos y programas informáticos (art. 197.3 CP) y a los delitos de daños de datos y de sistemas informáticos (art. 264.1 y art. 264. 2 CP). Asimismo, se formularán algunas breves consideraciones sobre las disposiciones que prevén la responsabilidad penal de las personas jurídicas. Finalmente, para concluir, se desarrollarán en perspectiva comparada algunas consideraciones críticas sobre la formulación de los nuevos delitos informáticos introducidos en el Código Penal español por la Ley Orgánica 5/2010.

Palabras clave: *Derecho Penal Informático, cibercrimen, intrusismo informático, daños informáticos, responsabilidad penal de las personas jurídicas, Convenio sobre Cibercrimen.*

ABSTRACT

In the present paper we will analyse the new offences against confidentiality, integrity and availability of data and computer systems, introduced into the Spanish Criminal Code trough the Organic Law No. (n.) 05/2010 of June 22, 2010 amending

Organic Law 10/1995, of November 23, on the Criminal Code. In particular, we will focus on the new offences concerning illegal access (art. 197 CP), data interference (art. 264.1 CP) and system interference (art. 264.2 CP) and the corporate liability. Finally, we will make some critical references about the legislative formulation of the new cybercrime offences introduced into the Spanish Criminal Code trough the Law 5/2010 in a comparative perspective.

Keywords: *Criminal Information law, cybercrime, illegal access, data and system interference, corporate liability, Cybercrime Convention.*

1. INTRODUCCIÓN

El 27 de noviembre de 2009 el gobierno español presentó un amplio proyecto de reforma de la Ley Orgánica 10/1995, de 23 de noviembre, esto es, al Código Penal vigente (1). El objetivo principal de la reforma, que en parte retomó el Anteproyecto de Ley Orgánica de 2008 (2), fue dar ejecución a las obligaciones internacionales y colmar las lagunas de punibilidad surgidas en la práctica, que por lo

(1) *Proyecto de Ley Orgánica por la que se modifica la Ley Orgánica* 10/1995, de 23 de noviembre, del Código Penal, 121/000052, disponible en la siguiente página web http://www.congreso.es/public_oficiales/L9/ CONG/BOCG/A/A_052-01.PDF. Para un primer comentario sistemático al mencionado proyecto de Ley Orgánica véase Álvarez García F. J., González Cussac J. L. (dirs.), *Consideraciones a propósito del proyecto de Ley de 2009 de modificación del Código Penal*, Valencia, 2010.

(2) *Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica* 10/1995, de 23 de noviembre, del Código Penal. Sobre las principales novedades previstas por el Anteproyecto de Ley Orgánica del 2008, de reforma del Código Penal v. Velasco Núñez E., «Delitos informáticos, terrorismo y derecho internacional en el Anteproyecto de Ley Orgánica de 2008, por la que se modifica la Ley Orgánica 10/1995, del Código Penal», en *La Ley Penal*, núm. 63, 2009, 5 ss.; Casanueva Sanz I., Pueyo Rodero J. A. (coord.), *El Anteproyecto de modificación del Código Penal de 2008: algunos aspectos*, Bilbao, 2009.

demás habían sido subrayadas hace tiempo por parte de la mejor doctrina. Además de la introducción de la responsabilidad penal de las personas jurídicas, el proyecto de reforma de 2009 previó la modificación de más de cientos de delitos del Código Penal, entre ellos los relativos a la explotación de menores, de combate al terrorismo, a la criminalidad organizada y al cibercrimen.

En referencia a la criminalidad informática, se previó la introducción en el Código Penal de un nuevo delito para castigar el fraude informático cometido mediante tarjetas de crédito y, en línea con las disposiciones de la Decisión Marco 2005/222/JAI, relativa a los ataques contra los sistemas de información, nuevas normas para castigar el acceso ilícito a un sistema informático (*hacking*) y los daños informáticos (3).

Después de una rápida tramitación legislativa, el proyecto gubernamental fue sometido al juicio de la Comisión de Justicia, siendo reenviado al Parlamento para su aprobación definitiva el día 29 de abril de 2010. Finalmente, dicho proyecto fue aprobado por el Senado el 22 de junio de 2010, convirtiéndose en la Ley Orgánica 5/2010 (4).

No obstante, conforme a la disposición séptima transitoria de dicha Ley Orgánica 5/2010, de 22 de junio, la cual apareció publicada en el Boletín Oficial del Estado al día siguiente, las modificaciones introducidas en el Código Penal entrarían en vigor tras una *vacatio legis* de seis meses, es decir, el 23 de diciembre de 2010.

Dada la extensión que posibilita el objeto del presente trabajo, limitaré mi atención a comentar los nuevos delitos informáticos en «sentido propio» (o *cyber crimes*) (5) introducidos por la mencionada Ley Orgánica 5/2010, sin tomar en consideración aquellos que pueden ser cometidos también a través de las redes informáticas

(3) «Proyecto de Ley Orgánica», cit., *Preámbulo*, XIV.

(4) Por un primer comentario sistemático a la Ley Orgánica 05/2010, v. Álvarez García F. J., González J. J. (dir.), «Comentarios a la Reforma Penal de 2010», Valencia, 2010; Ortíz de Urbina Gimeno, I., (coord.), «Memento Experto Reforma penal», Madrid, 2010; Quintero Olivares, G., (Dir.), La reforma Penal de 2010: Análisis y Comentario, Navarra, 2010. Sobre el contexto político-criminal de la Ley orgánica 05/2010 v. Silva Sánchez J. M., «La reforma del Código Penal: una aproximación desde el contexto», en *Diario La Ley,* núm. 7464, 9 de septiembre de 2010.

(5) Se hace referencia a aquellos delitos que pueden ser cometidos solamente en el ciberespacio a través de redes telemáticas. En doctrina v. las consideraciones de Sieber U., *Organised crime in Europe: the threat of cybercrime*, Council of Europe, Strasbourg, 2005, 86; también Picotti, L., «Biens juridiques protegès et techniques de formulation des infractions en droit pènal de l'informatique», in *Revue International de Droit Pènal*, vol. 77, 2006, 533.

(como por ejemplo el delito de *child grooming* o «ciber-acoso», del art. 183-bis *CP* (6), el de utilización ilícita de tarjetas de crédito del art. 248.2, let. c), CP, etc.) (7). Antes de proceder al análisis de las nuevas normas que protegen la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, se formularán algunas consideraciones sobre la peculiar ubicación sistemática que se les dio a los nuevos delitos informáticos en el Código Penal (párrafo 3). A continuación se revisarán las disposiciones del Código Penal de 1995 que, a falta de normas específicas, podían ser aplicadas por parte de los jueces para castigar la conducta no autorizada de acceso ilícito a un sistema informático y los denominados daños «funcionales» de sistemas informáticos (párrafos 3 y 5). El análisis de la normativa penal vigente permitirá evaluar si con la reforma legislativa de 2010 se han superado definitivamente aquellas lagunas que limitaban la posibilidad de castigar los más frecuentes ataques a los sistemas informáticos (*Hacking, Cracking, Denial of Service*, ecc.). Posteriormente se efectuará una referencia a la estructura de los nuevos tipos delictivos en materia de criminalidad informática. A este respecto se otorgará una especial atención a los delitos de acceso ilícito a datos y programas informáticos (párrafo 4) y a los delitos de daños de datos (párrafo 6) y de sistemas informáticos (párrafo 7). Asimismo, se formularán algunas breves consideraciones sobre las disposiciones que prevén la responsabilidad penal de las personas jurídicas (párrafo 8). Finalmente, para concluir, se desarrollarán algunas consideraciones críticas sobre la formulación de los nuevos delitos informáticos introducidos en el Código Penal español por la Ley Orgánica 5/2010, del 22 de junio (párrafo 9).

---

(6) Artículo 183-bis CP: «El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de trece años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 178 a 183 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño». Por un primer análisis del artículo 183-bis, CP, v. Vives Anton, T. S., Orts Berenguer, E., Carbonell Mateu, J. C., González Cussac, J. L., Martines-Bujan Pérez, C., *Derecho Penal, Parte especial*, III ed., Valencia, 2010, 269-271.

(7) Artículo 248.2, let. c) CP: «Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero».

2. LA UBICACIÓN SISTEMÁTICA DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ESPAÑOL

El legislador español introdujo en el Código Penal de 1995 algunos delitos específicos contra la criminalidad informática (8). En particular tipificó una serie de hechos ilícitos cometidos a través de o contra nuevos «objetos» informáticos y algunos actos preparatorios a la comisión de delitos más graves (en especial en referencia al fraude informático y a la violación de derechos de propiedad intelectual) (9).

La técnica de formulación normativa utilizada en el Código Penal de 1995 puede calificarse de muy peculiar, considerando que en lugar de crear tipos delictivos autónomos, como sucedió por ejemplo en Alemania (por la Ley 2. WiKG) (10) y en Italia (por la Ley 23 de diciembre de 1993, núm. 547), el legislador español prefirió modificar y extender el ámbito de aplicación de los delitos tradicionales (estafa, daños, etc.) que presentaban analogías con los nuevos actos ilícitos cometidos a través de las nuevas tecnologías.

---

(8) Con referencia a la relevancia penal de los delitos informáticos en la legislación penal española antecedente a la entrada en vigor del Código Penal de 1995 v., por todos, González Rus, J. J., «Aproximación al tratamiento penal de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos», en *RFDUCM*, Monográfico núm. 12, 1982, 107 ss.; Camacho Losa, L., *El delito informático*, Madrid, 1987; Romeo Casabona, C. M., *Poder informático y seguridad jurídica,* 1987, 90 ss.; Gutiérrez Francés, M. L., *Fraude informático y estafa*, Madrid, 1991; Corcoy Bidasolo, M., «Protección penal del sabotaje informático: especial consideración de los delitos de daños», en Mir Puig, S. (coord.), *Delincuencia informática*, Barcelona, 1992, 177 ss.

(9) Paradigmático es el artículo 248.3 CP, que castiga la fabricación, introducción, posesión y la puesta a disposición de programas informáticos específicamente destinados a la comisión de un fraude informático y el artículo 270.3 CP, que castiga la fabricación, la puesta en circulación y la posesión de medios destinados a neutralizar las medidas de seguridad puestas a protección de programas informáticos. Para un análisis del artículo 248.3 CP, v. Galán Muñoz, A., «El nuevo delito del artículo 248.3 CP: ¿un adelantamiento desmedido de las barreras de protección penal del patrimonio?», en *La Ley,* núm. 3, 2004, 1859 ss. Sobre el artículo 270.3 CP v. las consideraciones de Gómez Martín, V., «El delito de fabricación, puesta en circulación y tenencia de medios destinados a la neutralización de dispositivos protectores de programas informáticos (art. 270, párr. 3 CP). A la vez, un estudio sobre los delitos de emprendimiento o preparación con el CP de 1995», en *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 04-16 (2002), disponible en la siguiente página web http://criminet.ugr.es/recpc/recpc04-16.pdf; ID, «El artículo 270.3 CP: breve historia de un despropósito» en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. 21, 2007, 81 ss., con amplias referencias bibliográficas.

(10) «Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität» (2. WiKG), 15 de mayo de 1986, publicado en el *Bundesgesetzblatt*, núm. 21 de 23 de mayo de 1986 (BGBI 1986, I, 721).

La extensión de los tipos delictivos clásicos fue realizada de dos maneras. Por una parte, se introdujo dentro de los delitos tradicionales subtipos autónomos para castigar las nuevas modalidades ilícitas. Y por la otra, se amplió el ámbito de los objetos materiales de aquellos delitos que presentaban analogías con los nuevos hechos delictivos. De esta manera se tutelaron también los nuevos «objetos» informáticos (datos, programas y documentos informáticos) (11).

Un ejemplo paradigmático de la adopción de la primera técnica de formulación normativa es el delito de fraude informático (art. 248.2 CP) (12). Con respecto al delito tradicional de estafa (art. 248.1 CP) el «fraude informático», se realiza por parte del que obtiene un acto de disposición patrimonial mediante una conducta de tipo «lógico», es decir, a través de una manipulación informática u otro artificio semejante, que ocupa el lugar del engaño que induce a un tercero a error (13).

Un ejemplo de extensión del ámbito aplicativo de los delitos tradicionales mediante la introducción de nuevos objetos materiales es el delito de daños de datos, programas y documentos electrónicos contenidos en redes, soportes y sistemas informáticos (art. 264.2 CP), el cual se castiga como hipótesis agravada del delito de daños de cosas materiales (art. 263 CP) (14).

---

(11) Con referencia a la clasificación sistemática que distingue entre delitos informáticos según que el sistema informático constituya el objeto material del delito o el instrumento para la comisión de delitos, v. González Rus, J. J., *Aproximación al tratamiento penal de los ilícitos patrimoniales*, cit., 116 ss.; y, más reciente ID., «Protección penal de sistemas, elementos, datos, documentos y programas informáticos», en *Revista Electrónica de Ciencia Penal y Criminología*, RECPC 01-14 (1999), disponible al sitio http://criminet.ugr.es/recpc/recpc_01-14.html#1. Sobre las peculiaridades de esta técnica legislativa respecto a la que ha sido utilizada por otros legisladores europeos v. las consideraciones de Romeo Casabona, C. M., «Tendencias actuales sobre las formas de protección jurídica ante las nuevas tecnologías», en *Poder Judicial*, núm. 31, 1993, 180-181.

(12) Artículo 248.2 CP: «se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la trasferencia no consentida de cualquier activo patrimonial en perjuicio de tercero».

(13) Sobre la estructura del delito de fraude informático (art. 248.2 CP), v. Quintero Olivares, G., Morales Prats, F., Tamarit Sumalla, J. M., García Albero, R. (coords.), *Comentarios al Código Penal, Tomo II, Parte Especial*, V ed., Pamplona, 2008, 710-714; Queralt Jiménez, J. J., *Derecho Penal español*, Parte especial, VI ed., 2010, 517 ss.; Jiménez-Villarejo Fernández, F., «La delincuencia económica y las nuevas tecnologías: el fraude informático», en *Revista de Derecho Penal*, núm. 27, 2009, 11 ss.

(14) Artículo 264.2 CP: «La misma pena (pena de prisión de uno a tres años y multa de doce a veinticuatro meses) se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos

El esfuerzo del legislador de 1995 de integrar y adaptar lo máximo posible los nuevos delitos informáticos a los tipos delictivos tradicionales (estafa, daños, violación de secretos, etc.), pareció responder a la idea de que la llegada de las nuevas tecnologías hubiese comportado un cambio de las modalidades de agresión a los bienes jurídicos clásicos, recurriendo a la creación de artificiosas y poco apropiadas formulaciones legislativas y a una discutible ubicación sistemática de los nuevos delitos informáticos dentro del Código Penal.

Con la reforma de 2010 el legislador español, esencialmente en línea con la técnica adoptada en 1995, ha colocado los nuevos delitos informáticos que se refieren a la tutela de la confidencialidad, de la integridad y de la disponibilidad de los datos y sistemas informáticos al lado de aquellos tipos delictivos tradicionales que presentan respecto a ellos algunas (supuestas) analogías.

Paradigmática es en este sentido la (discutible) ubicación del nuevo delito de acceso ilícito a datos y programas informáticos (art. 197.3 CP) en el título X del Código Penal, que incluye los delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio.

A diferencia de lo que hizo el legislador en 1995, el de 2010 ha introducido los nuevos delitos de daños informáticos dentro de un tipo penal autónomo (art. 264 CP), en lugar de ponerlos al lado de las hipótesis agravadas del delito tradicional de daños de cosas materiales (art. 263 CP). Sin embargo, idéntica ha quedado la ubicación de la norma en el capítulo IX del título XIII, entre los delitos contra el patrimonio y el orden socioeconómico.

En los siguientes párrafos se subrayará como los nuevos delitos de acceso no autorizado a datos y programas informáticos y de daños informáticos, pese a su ubicación sistemática, tienen poco o nada que ver con los bienes jurídicos de la inviolabilidad del domicilio y del patrimonio.

---

electrónicos ajenos contenidos en redes, soportes o sistemas informáticos». Por un comentario, v. González Rus, J. J., «Daños a través de Internet», en AAVV, *Homenaje al Prof. Dr. G.R. Mourullo*, Navarra, 2005, 1469 ss., 1470-1477. Más en general, con referencia a las problemáticas jurídicas que presentan las conductas de daños informáticos, v. Camacho Losa, L., *El delito informático*, cit., 97 ss.; también, en perspectiva comparada Andrés Domínguez, A. C., «Los daños informáticos en la Unión Europea», en *La Ley*, núm. 1, 1999, 1724-1730; más reciente ID., «Los daños informáticos en el derecho penal europeo», en Álvarez García, F. J., Manjón-Cabeza Olmeda, A., Ventura Püchel, A. (coords.), *La adecuación del derecho penal español al ordenamiento de la Unión Europea: la política de la Unión Europea*, 2009, 411 ss.

3. LA IRRELEVANCIA PENAL DE LAS CONDUCTAS DE *HACKING* EN EL CÓDIGO PENAL DE 1995

A diferencia de lo que se había previsto en la mayoría de los ordenamientos jurídicos europeos, el legislador español de 1995, no consideró necesario castigar el acceso no autorizado a un sistema informático (*hacking*) (15).

A falta de una específica disposición penal sobre el *hacking*, según doctrina muy destacada, la intrusión ilícita en un sistema informático ajeno hubiera podido ser castigada en cuanto conducta instrumental a la comisión de determinados delitos informáticos, en particular los delitos de forma libre (16). Paradigmático era el artículo 197 CP, que no tipificando la modalidad de apropiación ilícita de mensajes de correo electrónico (art. 197.1 CP) o de datos de carácter personal o familiar contenidos en soportes informáticos o telemáticos (art. 197.2 CP), permite castigar aquellas violaciones de la intimidad que se realizan mediante la introducción ilícita en un ordenador ajeno (17). De igual manera se afirmó en referencia a los delitos de daños «lógicos» (art. 264.1 CP), que en ellos pueden ser subsumidas las conductas de acceso no autorizado que son instrumentales a la agresión de datos y programas informáticos (18). Por tanto, el simple acceso ilícito a un sistema informático hubiera sido ya penado en el ordenamiento jurí-

(15) En doctrina, v. De Alfonso Laso, D., *El hacker blanco. Una conducta ¿punible o impune?, en Internet y Derecho Penal, Cuadernos de Derecho Judicial*, Madrid, 2001, 514 ss.; Morón Lerma, E., *Internet y Derecho Penal: Hacking y otras conductas ilícitas en la Red,* Pamplona, 2002, 55 ss.; más reciente también González Rus, J. J., *Daños a través de Internet*, cit., 1481; ID., «Los ilícitos en la red (I): hackers, crackers, cyberpunks, sniffers, denegación de servicio y otros comportamientos semejantes», en Romeo Casabona, C. M. (coord.), *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006, 246; Rueda Martín, M. A., «Los ataques contra los sistemas informáticos: conducta de hacking. Cuestiones políticos-criminales», en *Sistema penal*, núm.1, 2008, 74. En la jurisprudencia, v. AP Tarragona, 23 de julio de 2001, JUR 310139/01.

(16) En este sentido, v. González Rus, J. J., «El *cracking* y otros supuestos de sabotaje informático», en *Estudios jurídicos, Ministerio Fiscal,* núm. 2, 2003, 246 ss.; ID., *Los ilícitos en la red (I),* cit., 246-247, según el cual: «a la postre, por tanto, lo que acaba decidiendo el carácter punible o no del acceso no autorizado a sistemas informáticos ajenos es la finalidad con la que el mismo se hace, resultando típico cuando, siendo un medio comisivo posible, el propósito del sujeto coincida con el del elemento subjetivo del injusto o el dolo propio de algún delito (...). El simple acceso no autorizado podrá resultar punible si constituye tentativa de los correspondientes delitos». Análogamente v. Morón Lerma, E., *Internet y Derecho Penal*, cit., 55.

(17) Cfr. Morón Lerma, E., *Internet y Derecho penal*, cit., 58-64.

(18) González Rus, J. J., *El cracking y otros supuestos de sabotaje informático*, cit., 223 ss.; id., González Rus, J. J., *Daños a través de Internet*, cit., 1482.

dico español, en cuanto constituya una tentativa de cometer una violación de la intimidad o un daño informático (19).

Mayores dudas han surgido en doctrina y en jurisprudencia en referencia a la posibilidad de castigar, a falta de una disposición específica, las conductas de simple acceso ilícito a un sistema informático realizadas sin finalidad ilícita ulterior (el llamado *«hacking* blanco*»)* (20). Una parte de la doctrina, ha afirmado la posibilidad de reconducir a estos hechos ilícitos el tipo delictivo de utilización no autorizada de un aparato de telecomunicación (art. 256 CP) (21).

El artículo 256 CP, que se encuentra en la sección III del capítulo VI del título XIII del mismo, entre «los delitos contra el patrimonio y el orden socioeconómico», castiga con la pena de multa de 3 hasta 12 meses «el que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a 400 euros».

En consecuencia, objeto material del delito tiene que ser un «equipo de telecomunicación», concepto que comprende todos aquellos aparatos por medio de los cuales se pueden establecer conexiones a distancia entre personas, ordenadores y redes de sistemas (por ejemplo, teléfonos, fax, correo electrónico, redes telemáticas, Internet, etc.) (22).

La conducta típica del artículo 256 CP consiste en utilizar un equipo de telecomunicación sin el consentimiento del legítimo titular. Esta se realiza tanto a través de la utilización no autorizada de un equipo ajeno, como cuando con su empleo se excede el ámbito de la autorización (23).

La «ratio» de la norma es la de castigar el llamado ««hurto de tiempo»», es decir, la utilización de servicios ofrecidos por un terminal (por ejemplo: navegación en Internet, consultación de bases de datos de pago, etc.) sin el consentimiento de su titular. Paradigmáticas

---

(19) En este sentido, v. González Rus, J. J., *Daños a través de Internet*, cit., 1482.

(20) Sobre la definición de *hacking «*blanco*»* como mero acceso no autorizado a un sistema informático sin alguna ulterior finalidad ilícita v. en jurisprudencia *Juzgado de lo Penal* núm. 2 de Barcelona, 28 de mayo de 1999, Fundamento jurídico 1 (cd. caso *Hispahack*). En doctrina, v. González Rus, J. J., *Los ilícitos en la red (I),* cit., 244.

(21) Cfr. Morón Lerma, E., *Internet y Derecho Penal*, cit., 55-58; González Rus, J. J., «Artículo 256 CP», en Cobo del Rosal, M. (coord.), *Comentarios al Código Penal*, Tomo VIII, Madrid, 2004, 555.

(22) En doctrina, v. Orts Berenguer, E., Roig Torres, M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia, 2001.

(23) En este sentido Quintero Olivares, G., Morales Prats, F., Tamarit Sumalla, J. M., García Albero, R. (coords.), *Comentarios*, cit., 771.

son las conductas de aquellos empleados (o *insider),* que utilizan de manera indebida los sistemas informáticos, los programas informáticos o la conexión a Internet de la empresa o de la hacienda pública para finalidades privadas o que exceden de las cargas laborales a las que están obligados.

La conducta de utilización no autorizada de un equipo será penalmente relevante si causa al titular del sistema un perjuicio económico superior a 400 euros. Por lo tanto, en el caso en que el sujeto haya utilizado, por ejemplo, el teléfono de la empresa para efectuar llamadas personales, o haya empleado sin autorización servicios de pago en red (por ejemplo bases de datos, etc.) para finalidades privadas, el juez tendrá que evaluar el coste económico de estos servicios empleados abusivamente (24).

Teniendo en consideración la ubicación sistemática y la formulación de la norma, la doctrina mayoritaria ha afirmado que el bien jurídico protegido por el artículo 256 CP es el patrimonio (25). Sin embargo, el carácter patrimonial del interés protegido por la norma impide subsumir en el artículo 256 CP la mayor parte de las conductas de acceso no autorizado a un sistema informático, puesto que estas no causan siempre un perjuicio económico al legítimo titular del sistema informático (26). Por lo tanto, el ámbito de aplicación del tipo delictivo se queda circunscrito a las conductas de utilización no consentida de determinados servicios, que se realizan en una fase temporalmente sucesiva a la de acceso ilícito a un sistema informático (27).

4. EL NUEVO DELITO DE ACCESO NO AUTORIZADO A DATOS Y PROGRAMAS INFORMÁTICOS (ART. 197.3 CP)

Para colmar las lagunas que no permitían castigar las conductas de *hacking* y *cracking*, el legislador español de 2010 ha introducido en el Código Penal una disposición *ad hoc* para sancionar el acceso no

(24) Cfr. Morón Lerma, E., *Internet y Derecho Penal,* cit., 57.

Sobre la escasa relevancia aplicativa de la norma debida también a las dificultades de determinar el perjuicio económico, v. González Rus, J. J., *Artículo 256 CP*, cit., 553.

(25) V., por todos, Orts Berenguer, E., Roig Torres, M., *Delitos informáticos,* cit., 76; Morón Lerma, E., *Internet y Derecho Penal*, cit., 56.

(26) Cfr. Morón Lerma, E., *Internet y Derecho Penal*, cit., 56; análogamente Gutiérrez Francés, M. L., *El intrusismo informático*, cit., 1174 ss.

(27) En este sentido v. Gutiérrez Francés, M. L., *El intrusismo informático*, cit., 1175; Morón Lerma, E., *Internet y Derecho Penal,* cit., 57.

autorizado a datos y programas informáticos (o «intrusismo informático*»).*

El nuevo párrafo tercero del artículo 197 CP castiga, con la pena de reclusión de 6 meses a dos años «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».

La formulación del nuevo delito de acceso no autorizado a datos y programas informáticos es muy similar a la del delito de violación de domicilio (art. 202 CP) (28). Muy similares son también las conductas típicas. El artículo 197.3 CP, de manera análoga al artículo 615.ter del Código Penal italiano (29), castiga dos hipótesis alternativas de conductas: aquella activa de quien «acceda sin autorización» a datos y programas informáticos contenidos en todo o en parte de un sistema informático y aquella omisiva de quien «se mantenga en el sistema contra la voluntad de quien tenga el legítimo derecho a excluirlo». Idéntico, respecto al delito de violación del domicilio, es el tratamiento sancionador (reclusión de 6 meses a 2 años).

La primera conducta que castiga el artículo 197.3 CP es la de acceso no autorizado a datos y programas informáticos. De esta manera se colma definitivamente la laguna que no permitía castigar el mero *hacking*.

En la mayoría de los casos, el acceso a datos y programas informáticos se verifica ya con la superación de las medidas de seguridad y la introducción en un sistema informático ajeno. La conducta de acceso tiene que ser entendida como la posibilidad por parte del sujeto agente de «utilizar» los datos sin que sea necesario que él se entere de su contenido (30).

---

(28) Artículo 202 CP: «1. El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años. 2. Si el hecho se ejecutare con violencia o intimidación la pena será de prisión de uno a cuatro años y multa de seis a doce meses».

(29) Artículo. 615-*ter,* comma 1, CP. *(«*accesso abusivo ad un sistema informatico o telematico»): *«Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni».*

(30) Sobre la interpretación de la conducta de «acceso» a un sistema informático, v. Salvadori, I., «L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking», en *Riv. it. dir. proc. pen*., núm. 3/2008, 1243 ss.

En concordancia con el artículo 2, párrafo 2, de la Decisión Marco 2005/222/JAH (esencialmente análogo al artículo 2, párrafo 2, del Convenio del Consejo de Europa sobre el cibercrimen) el nuevo artículo 197.3 CP requiere que la introducción no autorizada se realice mediante la violación de medidas de seguridad destinadas a impedir el acceso a los datos y a los programas informáticos contenidos en un sistema. En conformidad con el principio de *ultima ratio*, se evita de esta manera una excesiva extensión del tipo delictivo, ya que se requiere como condición para la intervención penal que el titular haya dispuesto una protección de naturaleza técnica y que ésta se haya demostrado suficiente.

De forma análoga a otros legisladores europeos (por ejemplo al alemán, austríaco, italiano, etc.), el legislador español no ha definido el concepto técnico de medidas de seguridad (31). Faltando una definición expresa, la locución tiene que ser interpretada en sentido amplio para comprender todo tipo de barrera u obstáculo puesto para la protección de datos y de programas informáticos, si bien con un grado mínimo de eficacia (32). Las medidas de seguridad pueden tener naturaleza «física» o «lógica». En consecuencia, dentro de ellas se incluyen tanto medios físicos para el encendido (como claves), como de naturaleza organizativa (colocación del ordenador en un sitio cerrado), hasta los medios técnicos más sofisticados de identificación del usuario (por ejemplo palabras claves, secuencias numéricas, huellas digitales, datos biométricos, etc.), que permiten excluir a personas no autorizadas del acceso a datos y programas informáticos.

Además de la conducta activa de acceso no autorizado a datos y programas informáticos, el artículo 197.3 CP castiga la conducta omisiva del «mantenerse» en un sistema contra la voluntad del legítimo titular (33). El objetivo de esta previsión, que está contemplada tam-

(31) Diferente ha sido la elección del legislador rumano, que yendo más allá del artículo 1 del Convenio sobre el cibercrimen, en el artículo 35, let. h), de la Ley 21 de abril de 2003, núm. 161, ha definido la noción de medidas de seguridad como aquel conjunto de «procedimientos, aparatos o programas informáticos específicos por medio de los cuales el acceso a un sistema informático está restringido o prohibido a determinadas categorías de sujetos».

(32) Análogamente v., en la doctrina alemana Hilgendorf, E., «§ 202a StGB», *Leipziger Kommentar*, 2010, 1448-1449, Rdnúm. 34; KARGL W., «§ 202a StGB», in Kindhäuser, U., Neumann, U., Paeffgen, H.-U. (Hrsg.), *Strafgesetzbuch, Nomoskommentar*, Band 2, 3. Auf., 2010, 486.

(33) Con referencia a la análoga hipótesis del «mantenerse» en un sistema informático, prevista por el artículo 615-ter del Código Penal italiano v. Pecorella C., *Il diritto penale dell´informatica*, Padova, 2006, 349-352. Sobre el carácter omisivo de esta conducta v. también Mucciarelli, F., «Commento agli art. 1,2,4 e 10 l. 1993 núm. 547», en *Legisl. Pen*., 1996, 100; Picotti, L., «voce Reati informatici», en *Enci-*

bién en el Código Penal italiano (art. 615-*ter CP*), parece castigar aquellas hipótesis muy frecuentes en la práctica en las que, después de una inicial introducción obtenida de manera legítima o casual, el sujeto agente se «mantiene» en el sistema ajeno contra la voluntad de quien tiene el derecho de excluirlo.

La conducta (alternativa) de mantenerse en un sistema incluiría, por lo tanto, las hipótesis omisivas de la «parada» o de la «permanencia» abusiva en un sistema informático, que no podrían ser de otra manera subsumidas en la conducta activa de «acceso» no autorizado. Esta conducta no tendrá que entenderse en sentido «físico», sino como mantenimiento de la conexión, inicialmente obtenida de manera autorizada o fortuita, a todo o en parte de un sistema de información. Lo que se castiga por lo tanto es la «permanencia» *invito domino* en el sistema informático ajeno realizada por quien, por casualidad o teniendo al principio la autorización del legítimo titular, haya seguido manteniéndose en el sistema informático pese a que se haya acabado el consentimiento de aquello.

Con la permanencia no autorizada en un sistema ajeno surge el peligro que el agente o aquellos sujetos que se encuentran cercanos de aquel sistema informático puedan aprovechar su carácter temporalmente abierto para acceder sin autorización a los datos y programas informáticos que están contenidos en el mismo o que son accesibles a través del mismo.

Paradigmático es el caso del técnico informático, que siendo autorizado a acceder a un ordenador para verificar su correcto funcionamiento, se mantiene conscientemente más allá del tiempo necesario para efectuar el mencionado control. De esta manera surgiría el riesgo de que el técnico informático pueda realizar ulteriores actividades no autorizadas (por ejemplo copiar datos, controlar archivos, etc.), contrarias a aquellas por las que estaba inicialmente autorizado (34).

Piénsese también en el profesional que no pudiendo conectarse a Internet, entrega a su secretaria las credenciales de acceso a su cuenta personal de correo electrónico para que ella verifique el horario de una cita o de un asunto profesional. En el caso en que la secretaria, después de haber controlado el correo electrónico de su jefe de tra-

---

clopedia Giuridica Treccani, Aggiorn., Roma, 2000, 22. Contra Pica, G., *Diritto penale delle tecnologie informatiche,* Torino, 1999, 42, según el cual la de «mantenerse» es una conducta de acción que perdura con consentimiento y por lo tanto comisiva, puesto que la norma no se centra en la sanción de la falta de abandono del sistema, sino en el mantenimiento voluntario del acceso al sistema informático.

(34) En este sentido v. también Carrasco Andrino, M., «El delito de acceso ilícito a los sistemas informáticos», en Álvarez García, F. J., González Cussac, J. J. (dir.), *Comentarios*, cit., 254.

bajo, se ponga sin ser autorizada a mirar otros correos o no proceda a cerrar voluntariamente la cuenta de correo, ella se mantendrá abusivamente en el sistema informático.

Por la formulación del artículo 197.3 CP hay que considerar que también la hipótesis de la permanencia tiene como objeto un sistema informático «protegido» por medidas de seguridad. El sujeto agente tendrá que ser consciente de encontrarse dentro de un espacio protegido del sistema informático. Para la consumación del tipo delictivo no será necesario que el sujeto haya sobrepasado ilícitamente las medidas de protección, siendo esta última conducta ya subsumible en la hipótesis activa de acceso no autorizado a datos y programas informáticos.

El delito se consuma respectivamente con el acceso a datos y a programas informáticos o cuando se acaba el «plazo» establecido para «salir» del sistema informático en el que los datos y los programas están contenidos. Este «plazo», que establece el momento a partir del cual la conducta omisiva del «mantenerse» tiene que ser considerada típica, tendrá que ser establecido en base a las normas extrapenales (por ejemplo: contrato de trabajo, contrato individual, usos empresariales, costumbres, etc.), que disciplinan la actividad del sujeto que opera sobre el sistema informático o sobre la base de la autorización (explícita o tácita) concedida a este sujeto por parte del legítimo titular del derecho de excluirlo.

Pese a su ubicación sistemática en el título X del Código Penal, entre los «delitos contra la intimidad, la propia imagen y la inviolabilidad del domicilio y de la intimidad», la norma no tutela (solamente) el formal interés del legítimo titular a la intimidad de los datos o programas informáticos contenidos en un sistema. Mejor dicho, la disposición protege el poder del titular del derecho a excluir a otros (o *ius excludendi alios*) de disponer de manera exclusiva de sus datos y programas informáticos, independientemente de su contenido (secreto o reservado) o de su valor económico (35).

(35) En este sentido v. ya en la doctrina extranjera SIEBER, U., *The International Handbook*, cit., 86; ID., «Computerkriminalität und Informationsstrafrecht», *CR,* 1995, 103; ID., en HOEREN, T., SIEBER, U. (Hrsg.), *Handbuch Multimedia- Recht*, München, 2009, 418; en la doctrina española, v. GALÁN MUÑOZ, A., «La internacionalización de la represión y la persecución de la criminalidad informática: un nuevo campo de batalla en la eterna guerra entre prevención y garantías penales», en *Revista Penal,* núm. 24, 2009, 95. Individualiza el bien jurídico protegido por el delito de acceso no autorizado a un sistema informático como la «integridad» de los sistemas informáticos GERCKE, M., «Die Cybercrime Konvention», en *Computer und Recht International,* 2004, 729. Sobre este tema v. también SALVADORI, I., *L'esperienza giuridica*, cit., 1281.

Conforme a lo establecido en el artículo 7, párrafo 1, de la Decisión Marco 2005/222/JAI, el legislador español ha previsto un aumento de pena respecto a la hipótesis básica del artículo 197.3 CP, en el presupuesto en que el acceso no autorizado haya sido cometido en el marco de una organización o de un grupo criminal (art. 197.8 CP).

El nuevo artículo 570-*bis* CP, introducido por la Ley Orgánica 05/2010, establece que a los efectos del Código Penal se entiende por organización criminal «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, así como de llevar a cabo la perpetración reiterada de faltas» (36).

Por su parte, el nuevo artículo 570-*ter* CP establece que para los efectos del Código Penal constituye un grupo criminal «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 o la comisión concertada y reiterada de faltas» (37).

5. LOS DELITOS DE DAÑOS INFORMÁTICOS EN EL CÓDIGO PENAL ESPAÑOL DE 1995

Con el fin de superar las lagunas que no permitían castigar los daños a datos y programas informáticos (o daños «lógicos»), el legislador español introdujo en el Código Penal de 1995 un tipo delictivo específico: el «sabotaje informático» (38).

El artículo 264.2 CP, ubicado en el capítulo IX, dentro de los delitos comunes de daños, castigaba con la pena de reclusión de 1 a 3 años y multa de 12 a 24 meses al «que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o docu-

(36) Sobre el concepto legal de organización criminal v. García Rivas, N., Lamarca Pérez, C., «Organizaciones y grupos criminales», en Álvarez García, F. J., González Cussac, J. J. (direc.), *Comentarios*, cit., 507-508.

(37) Sobre el concepto legal de grupo criminal v. García Rivas, N., Lamarca Pérez, C., «Organizaciones y grupos criminales», in Álvarez García, F. J., González Cussac, J. J. (direc.), *Comentarios*, cit., 510-512.

(38) Sobre las tentativas jurisprudenciales y doctrinales de reconducir a falta de una norma específica los daños informáticos en los comunes tipos delictivos del Código Penal anterior al de 1995 v., por todos, Corcoy Bidasolo, M., *Protección penal del sabotaje informático,* cit., 160 ss.; González Rus, J. J., *Aproximación al tratamiento penal*, cit., 197 ss., con amplias referencias bibliográficas.

mentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos».

La doctrina mayoritaria evaluó positivamente la previsión de un tipo penal autónomo de daños informáticos, atendido que permitía castigar aquellas agresiones a los nuevos «objetos» informáticos (datos, informaciones y programas), que no podían ser subsumidos en el delito común de daños en propiedad ajena (art. 263 CP). El principal obstáculo a la posibilidad de reconducir en el tradicional delito de daños a «cosas» las agresiones a los nuevos «objetos» informáticos, era representado por la peculiar naturaleza inmaterial de estos últimos objetos (39).

Un sector de la doctrina había considerado inútil y prescindible la introducción en el Código Penal de 1995 del artículo 264.2 CP, dado que estimaba que las conductas de daños «lógicos» habrían podido ser pacíficamente reconducidas en el delito común de daños (40). Este último, –señalaba este sector– contrariamente, por ejemplo al tipo delictivo de daños previsto por el artículo 635 del Código Penal italiano (41), no requería expresamente un daño a una «cosa» material, sino a la «propiedad» ajena (42). Por lo tanto, era suficiente para su consumación que el objeto material sobre el que tenía que recaer la conducta agresiva pudiera ser dañado, alterado o hecho inutilizable, prescindiendo de su naturaleza corporal o material (43).

El hecho típico del artículo 264.2 CP consistía en «destruir, alterar, hacer inutilizable o dañar en cualquier otro modo» datos y programas informáticos o documentos electrónicos. El tipo delictivo castigaba no solamente los daños «lógicos», sino también aquellos

(39) En este sentido v. Corcoy Bidasolo, M., *Protección penal del sabotaje informático*, cit., 145 ss.; Orts Berenguer, E., Roig Torres, M., *Delitos informáticos*, cit., 78; Andrés Domínguez, A. C., «El delito de daños en la Unión Europea», en *La Ley*, n.1, 1999, 31.

(40) González Rus, J. J., *Aproximación al tratamiento penal,* cit.

(41) Artículo 635, comma 1, CP *(danneggiamento)*: «Chiunque distrugge, disperde, deteriora o rende, in tutto o in parte, inservibili cose mobili o immobili altrui, è punito, a querela della persona offesa, con la reclusione fino a un anno o con la multa fino a euro 309».

(42) En este sentido v. ya González Rus, J. J., *Aproximación al tratamiento penal,* cit., 178 ss.; ID., «Naturaleza y ámbito de aplicación del delito de daños en elementos informáticos (art. 264.2 del Código Penal)», en AA.VV., *La ciencia del Derecho Penal ante el nuevo siglo. Libro Homenaje al profesor Doctor José Cerezo Mir*, Madrid, 2002, 1285 ss. En términos similares, Romeo Casabona, C. M., *Tendencias actuales,* cit., 104 ss.; Gutiérrez Francés, L. M., «Delincuencia económica e informática en el nuevo Código Penal», en AA.VV., *Ámbito jurídico de las tecnologías de la información,* en *Cuadernos de Derecho Judicial,* Madrid, 1996, 295.

(43) González Rus, J. J., *Aproximación al tratamiento penal,* cit., 138-142.

«físicos» cometidos contra suportes materiales que contenían los mencionados «objetos» informáticos (44). Los daños que se cometían directamente contra una parte física (o *hardware*) de un sistema (por ej. teclado, pantalla, impresora, etc.) se castigaban a través del delito tradicional de daños de cosas (art. 263 CP).

Los objetos materiales del delito eran los «datos, programas o documentos informáticos» (45). En particular la conducta violenta de daños tenía que recaer sobre datos, documentos y programas informáticos contenidos en un soporte físico (por ej. CD, DVD, tarjetas magnéticas, etc.), archivados o almacenados en un sistema informático o en fase de transmisión en red (por ej. a través de Internet, WI-FI, etc.).

El legislador español de 1995 limitó la tutela penal solamente a datos y programas informáticos y documentos electrónicos «ajenos». Según parte de la doctrina, el propietario de estos «objetos» no podría ser considerado sujeto activo del delito (46). Sin embargo, esta interpretación en clave civilista del concepto de «ajenidad» sería demasiado restrictiva, porque llevaría a la absurda consecuencia de excluir del ámbito de la tutela penal aquellos sujetos que tienen un derecho de usufructo sobre los datos y los programas informáticos y que tienen un legítimo interés a su integridad y disponibilidad, pese a no ser propietarios en sentido civilístico.

6. EL NUEVO DELITO DE DAÑOS DE DATOS INFORMÁTICOS (ART. 264.1 CP)

Con el objetivo de dar plena transposición a las disposiciones de la Decisión Marco 2005/222/JAH sobre *data interference* y *system interference* y de superar los evidentes límites del artículo 264.2 CP, que no permitían sancionar las siempre más peligrosas formas de ataques a

(44) Cfr. Orts Berenguer, E., Roig Torres, M., *Delitos informáticos*, cit., 79.

(45) Sobre la definición de los objetos materiales típicos del artículo 264.2 CP v. González Rus, J. J., *Daños a través de Internet*, cit., 1473 ss.

(46) Cfr. González Rus, J. J., *Daños a través de Internet,* cit., 1477; Corcoy Bidasolo, M.., «Problemática de la persecución de los denominados delitos informáticos: particular referencia a la participación criminal y al ámbito espacio temporal de comisión de los hechos», en *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, núm. 21, 2007, 17 Análogamente v. en la doctrina italiana, con referencia al hoy abrogado artículo 635-*bis* CP introducido por la Ley núm. 547/1993, Mantovani, F., «Danneggiamento di sistemi informatici e telematici», en *Dig. disc. pen., vol.* agg., Torino, 2004, 172, que excluye la configuración de un delito de daño de datos informáticos cometido por el propietario a daño del titular de un derecho de usufructo sobre la cosa dañada.

los sistemas informáticos que se cometen a través de Internet (por ej. ataques *Denial of service, Netrike*, *Spamming*, etc.) (47), con la Ley Orgánica 5/2010, el legislador español ha introducido en el Código Penal dos nuevas figuras delictivas en materia de daños informáticos.

La primera de ellas es el nuevo delito de daños de datos informáticos (art. 264.1 CP) que esencialmente asume el contenido del artículo 4 de la Decisión Marco 2005/222/JAH, castigando con la pena de reclusión de 6 meses a 2 años al que «por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave».

Respecto al hoy derogado artículo 264.2 CP, el legislador español de 2010 ha previsto en el hecho típico del nuevo artículo 264.1 CP, las hipótesis de «borrar», «deteriorar» y «suprimir» y «hacer inaccesibles» datos y programas informáticos o documentos electrónicos. Se trata de «resultados», que en parte se sobreponen entre ellos, evitando de esta manera que en el futuro puedan surgir riesgos de una eventual laguna de protección por la aparición de nuevas formas de agresión a datos informáticos.

El resultado típico de «borrar», que corresponde a la destrucción de un objeto corporal o material puede realizarse no solamente a través del formateo de soportes, sino también a través de la destrucción o el daño del mismo soporte físico en el que están contenidos (48). Desde un punto de vista penal será absolutamente irrelevante el hecho de que los datos informáticos borrados puedan ser recuperados por parte del sujeto que tiene un derecho sobre otro soporte (por ejemplo CD-ROM, copia de *back-up*, *Server*, etc.).

El «deteriorar», que en parte se sobrepone con la hipótesis de dañar, tendrá que ser entendido como un menoscabo de la integridad o del contenido informativo de datos o programas informáticos.

La «supresión» consiste en impedir al titular de los datos acceder de manera tanto permanente como temporal a datos informáticos. Este resultado puede realizarse a través de un traslado de datos a un directorio diferente, o mediante la «ocultación», la mera sustitución o

(47) Para un análisis de la relevancia penal de estas conductas en el ordenamiento jurídico italiano v. SALVADORI, I., Hacking, cracking «e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de jure condendo», en *Cyberspazio e diritto*, núm. 3, 2008, 329 ss.

(48) En este sentido v., con referencia al análogo delito de daños de datos informáticos previsto por el § 303a del Código Penal alemán HILGENDORF, E., FRANK, T., VALERIUS, B., *Computer und Internetstrafrecht*, Berlin, Heidelberg, 2005, 55; TOLKSDORF, K., *§ 303a StGB*, *Leipziger Kommentar*, 2010, 55.

modificación del nombre del archivo en el que son contenidos aquellos o por medio de la sustracción del soporte en el que están archivados (49).

El «hacer inaccesibles» datos o programas informáticos abarca toda acción que obstaculiza de manera permanente o temporal la disponibilidad y la correcta utilización de los datos informáticos por parte del «titular» del derecho. De esta manera pueden ser sancionadas también aquellas conductas que a pesar de no causar un daño (por ejemplo a través su cancelación, supresión o deterioro), impiden al que tiene un legítimo derecho de disposición (propietario, posesor, etc.), acceder y utilizar de manera regular los datos y los programas informáticos.

En conformidad con el artículo 3 de la Decisión Marco 2005/222/JAH, el legislador español ha limitado el ámbito aplicativo del tipo delictivo a los casos en que el resultado producido a través del daño sea grave. La *ratio* de esta elección es la de restringir el hecho típico, que de otra manera sería lo suficientemente amplio para abarcar incluso la mera alteración de aquellos datos que no tienen ningún valor o utilidad.

Faltando una definición legal del elemento «elástico» o «indefinido» de la gravedad del resultado de daño, tocará a los jueces la tarea de especificar el parámetro para seleccionar aquellos resultados que son penalmente relevantes (50). La previsión de esta locución indeterminada produce fuertes perplejidades con referencia al respeto del fundamental principio de taxatividad.

De forma totalmente pleonástica, el artículo 264.1 CP, requiere también que los hechos típicos de daño de datos y programas informáticos y de documentos electrónicos sean cometidos «de manera grave».

La norma requiere al mismo tiempo que las conductas de daño de datos tienen que ser penadas solamente si se cometen sin autorización: locución que equivale a la de «sin derecho» establecida en el Convenio del Consejo de Europa sobre el cibercrimen (art. 5) y en la Decisión Marco 2005/222/JAH (art. 4). Al lado de esta oportuna cláusula de ilicitud expresa, el legislador español ha mantenido de manera

---

(49) Afirma que estas conductas no pueden ser subsumidas en el tipo delictivo de daño del artículo 264.2 CP, puesto que no determinan alguna alteración de la substancia de los elementos lógicos: González Rus, J. J., *Los ilícitos en la red*, cit., 264.

(50) Teniendo en cuenta la ubicación de la norma entre los delitos contra el patrimonio y el orden socioeconómico, afirma que la gravedad del resultado dañoso tiene que referirse al valor patrimonial de los objetos materiales (datos, programas o documentos informáticos) dañados: Muñoz Conde, F., *Derecho Penal, Parte Especial*, XVIII ed., Valencia, 2010, 480.

errónea el requisito de la «ajenidad» de los datos, programas y documentos electrónicos. De esta manera el ámbito de los sujetos pasivos queda limitado una vez más a los propietarios o por lo menos a los poseedores de los «objetos» inmateriales dañados.

Idéntico a lo del artículo 264.2 CP, introducido en el Código Penal del 1995, es el objeto pasivo del nuevo tipo delictivo de daños de datos informáticos del artículo 264.1 CP. Completamente redundante es la previsión junto a los datos y a los programas informáticos, de los documentos electrónicos, que constituyen un conjunto de datos informáticos creado a través de un procedimiento de elaboración de datos.

En conformidad con lo que establece el artículo 7, párrafo 1 y 2, de la Decisión Marco 2005/222/JAI, la Ley Orgánica 05/2010 introduce un nuevo párrafo al artículo 264 CP, para castigar de manera agravada los daños cometidos en el marco de una organización criminal (art. 264.3.1, CP), y el supuesto en que se produzcan «daños de especial gravedad» o que afecten «intereses generales» (51).

Esta previsión produce fuertes dudas en referencia al respeto del principio de taxatividad, en la parte en que castiga de forma más severa las agresiones a datos que causan «daños de especial gravedad». Si la gravedad de los resultados de daño constituye ya un elemento típico de la hipótesis básica del artículo 264.1 CP, insalvables dificultades prácticas podrían surgir a la hora de distinguir entre las hipótesis que lesionan de manera grave los datos informáticos respecto de aquellas (agravadas) que causan un daño de especial gravedad. Desde una perspectiva de *lege ferenda* será oportuno que el legislador español modifique la formulación del tipo delictivo u ofrezca criterios para definir de manera más precisa esta locución indeterminada.

Al mismo tiempo, imprecisa resulta ser la formulación del artículo 264.3 CP, allí donde castiga de manera agravada el daño que afecta a «intereses generales». Una correcta interpretación de la locución podría llevar a subsumir en la mencionada hipótesis todos aquellos casos en que la agresión a datos informáticos lesionan intereses públicos o de la colectividad o que incidan sobre el regular funcionamiento de las infraestructuras críticas (por ej. el tráfico aéreo, naval o ferroviario, estructuras hospitalarias, centros nucleares, etc.), cuyo

(51) Artículo 264.3 CP: «3. Se impondrán las penas superiores en grado a las respectivamente señaladas en los dos apartados anteriores y, en todo caso, la pena de multa del tanto al décuplo del perjuicio ocasionado, cuando en las conductas descritas concurra alguna de las siguientes circunstancias: 1. Se hubiese cometido en el marco de una organización criminal. 2. Haya ocasionado daños de especial gravedad o afectado a los intereses generales».

correcto funcionamiento depende cada vez más de la integridad y de la regular disponibilidad de los datos y de los sistemas informáticos.

A pesar de la ubicación entre los delitos contra el patrimonio y el orden socioeconómico, el bien jurídico protegido por el nuevo delito de daños de datos informáticos tendrá que ser individualizado, de conformidad con las indicaciones de fuente internacional (52), como el interés del legítimo titular a la plena disponibilidad e integridad de los datos y de los programas informáticos (53).

7. EL NUEVO DELITO DE DAÑOS DE SISTEMAS INFORMÁTICOS (ART. 264.2 CP)

Con el objetivo de ejecutar la obligación de incriminar las conductas de *system interference,* requerida por el artículo 3 de la Decisión Marco 2005/222/JAH, el legislador español de 2010 ha introducido un nuevo párrafo segundo en el artículo 264 CP. El nuevo delito de daño de sistemas informáticos castiga con la pena de prisión de seis meses a tres años al 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».

El artículo 264.2 CP constituye una disposición que contiene diversos tipos delictivos. El primer tipo delictivo castiga el daño de un sistema informático cometido mediante uno de los «hechos» típicos establecidos por el artículo 264.1 CP, es decir, el «borrar, dañar, deteriorar, alterar, suprimir o hacer inaccesible» datos informáticos, cuando produzca el efecto de obstaculizar el funcionamiento del sistema.

La segunda previsión castiga el sabotaje informático cometido mediante las conductas de «introducción» o «trasmisión» de datos informáticos en un sistema informático. Esta comprensible previsión, que resulta ser conforme no solamente a las fuentes supranacionales,

(52) En particular v. Conseil de L'europe, *La criminalitè informatique. Recommandation n. R (89) 9 sur la criminalitè en relation avec l'ordinateur. Rapport final du Comitè europèen pour les problèmes criminels*, Strasbourg, 1990, 44; Council of Europe, *Convention on Cybercrime, Explanatory Report*, 60.

(53) En este sentido v. ya Corcoy Bidasolo, M.., *Protección penal*, cit. En contra, González Rus, J. J., *Naturaleza y ámbito de aplicación*, cit., 1293, 1294, según el cual el bien jurídico tutelado tiene que ser individualizado como la propiedad del titular de los datos dañados.

sino también a las de muchos ordenamientos jurídico-penales europeos (véase por ejemplo el § 303b del Código Penal alemán (54), el art. 635-*quater* del Código Penal italiano (55), etc.) permite castigar las cada vez más frecuentes conductas de *Net-Strike y Mail-Bombing*, la introducción o trasmisión de programas *malware* o de mensajes de correo electrónico no deseados (o *spam*), cuyo efecto es interferir de manera grave en el correcto funcionamiento de un sistema de información (56).

Comprensible es la elección del legislador español de castigar solamente aquellas conductas que causan un daño «grave». De esta manera se restringe el ámbito de aplicación del tipo delictivo y se evita el recurso a la sanción penal para castigar hechos típicos que presentan una relevancia solamente bagatelar y que pueden ser resueltos sin un excesivo gasto de tiempo y de dinero. Sin embargo, es esta una cláusula elástica o indeterminada, que levanta perplejidades en referencia al respeto del principio de taxatividad, puesto que el legislador español no ha provisto de un criterio legal para seleccionar las hipótesis de daño grave. Por lo tanto, será tarea de cada juez determinar las hipótesis de daño que resultan ser penalmente relevantes.

Análogamente a lo que establece el artículo 3 de la Decisión Marco 2005/222/JAH, el resultado típico del artículo 264.2 CP consiste en «obstaculizar o interrumpir el funcionamiento» de un sistema informático ajeno. De esta manera se supera la laguna que imposibilitaba la subsunción en el artículo 264.2 CP de las conductas que causan un daño solamente «funcional» a un sistema informático (por ejemplo a través de ataques *Denial of service* o *Mail-bombing*).

Algunas dudas surgen sobre la posibilidad de reconducir al artículo 264.2 CP los daños informáticos «físicos», es decir, aquellos daños cometidos a través de ataques a la parte *hardware* de un sistema

---

(54) § 303b.1 StGB (*Computersabotage*): «(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er 1. eine Tat nach § 303a Abs. 1 begeht, 2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder 3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft»

(55) Artículo 635-*quater* CP: («Danneggiamento di sistemi informatici o telematici»): «Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni».

(56) Sobre estas nuevas formas de ataques a la integridad y la disponibilidad de los datos y de los sistemas informáticos v. SALVADORI, I., *Hacking, cracking,* cit., 329-369.

informático. En efecto no se trata de un delito de resultado a conducta libre, sino vinculada, puesto que la norma sanciona la interrupción o la interferencia en el correcto funcionamiento de un sistema informático, solamente si se cometen a través de un daño a los datos informáticos. También los ataques «físicos» a un sistema informático podrán ser subsumidos en el artículo 264.2 CP, pero solamente si causan de manera indirecta un daño a datos y a programas informáticos contenidos en el mismo sistema. En cambio, los daños a la parte física (o *hardware*) de un sistema informático, que no afecten su correcto funcionamiento, tendrán que ser subsumidos en el delito común de daño en la propiedad ajena (art. 263 CP). Sin embargo, esto implica una evidente disparidad de tratamiento desde el punto de vista sancionador, puesto que hechos ilícitos de análogo disvalor, en cuanto lesivos del mismo interés jurídico de la integridad y de la disponibilidad de sistemas informáticos, serán castigados de manera diferente, según la naturaleza «física» (art. 263 CP: pena de multa de 6 a 24 meses) o «lógica» (art. 264.2 CP: pena de reclusión de 1 a 3 años) de las modalidades agresivas.

Al igual que en el delito de daños de datos informáticos, el legislador español ha previsto un aumento de pena, respecto a la hipótesis básica del artículo 264.2 CP, para los sabotajes informáticos cometidos en el ámbito de una organización criminal (art. 264.3.1. CP), y para aquellos que causen daños de especial gravedad o que afectan a intereses generales (véase *supra* párrafo 6).

8. LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS POR LOS DELITOS INFORMÁTICOS

A pesar de la fuerte resistencia de la doctrina, el legislador español del 2010, en conformidad con las indicaciones internacionales y con las normas de muchos ordenamientos europeos (por ejemplo: francés, holandés, belga, portugués, noruego e italiano) ha superado definitivamente el principio *societas delinquere non potest* introduciendo en el Código Penal la responsabilidad penal de las personas jurídicas (57).

(57) Sobre los presupuestos para la responsabilidad penal de las personas jurídicas en el debate doctrinal español v., entre todos, Bacigalupo, S., *La responsabilidad penal de las personas jurídicas*, Barcelona, 1998; Hurtado Pozo, J., Del Rosal Blasco, B., Simons Vallejo, R. (coords.), *La responsabilidad penal de las personas jurídicas: una perspectiva comparada*, Valencia, 2001; Mir Puig, S., «Una tercera vía en materia de responsabilidad penal de las personas jurídicas», en *RECPC*, 06-01 (2004), disponible a la siguiente página web http://criminet.ugr.es/recpc/06/recpc06-

El nuevo artículo 31-bis CP prevé un doble criterio de imputación de la responsabilidad penal de las personas jurídicas, inspirado en el modelo de la llamada responsabilidad vicarial (58). La responsabilidad penal del ente se basa en la comisión de un delito por parte de una o más personas físicas pertenecientes a determinadas categorías.

En base al artículo 31-bis.1, primer inciso, CP, el ente colectivo es penalmente responsable por los delitos cometidos por parte de sus representantes legales, del administrador de derecho o de hecho que hayan actuado en nombre o por cuenta o en beneficio del mismo ente. La persona jurídica responde además por los delitos cometidos por sujetos «subordinados» en el ejercicio de actividades sociales y por cuenta, y en provecho de la misma cuando los hechos se hayan podido realizar por la falta de control de la persona jurídica sobre su actuación (art. 31-*bis*.1, segundo inciso, CP).

En el Código Penal español no se ha introducido un modelo de culpabilidad de organización en la reglamentación de la responsabilidad penal de las personas jurídicas. El artículo 31-*bis* CP requiere solamente de una omisión de los deberes de control y vigilancia correspondientes a la persona jurídica cuando la actividad delictiva se cometa por parte de un sujeto subordinado. En definitiva este sistema de imputación de responsabilidad penal a las personas jurídicas no prevé el posible déficit de estructura organizativa. es decir, de una cul-

---

01.pdf; Nieto Martín, A., *La responsabilidad penal de las personas jurídicas: un modelo legislativo*, Madrid, 2008; Carbonell Mateu, J. C., «Aproximación a la dogmática de la responsabilidad penal de las personas jurídicas», en Carbonell Mateu, J. C., González Cussac, J. J., Orts Berenguer, E., Cuerda Arnau, M. L. (coords.), *Constitución, derechos fundamentales y sistema penal*, Valencia, 2009, 307 ss.; Morales Prats, F., «La evolución de la responsabilidad penal de las personas jurídicas en Derecho español: de lo accesorio a lo principal», en Muñoz Conde, F.J. (coord.), *Problemas actuales del derecho penal y de la criminología: estudios penales en memoria de la profesora Dra. María del Mar Díaz Pita*, Valencia, 2008, 595 ss. En referencia a los presupuestos de la responsabilidad introducida por la Ley 05/2010 v. en sentido crítico Bacigalupo Zapater, E., «Responsabilidad penal y administrativa de las personas jurídicas y programas de *compliance* (A propósito del Proyecto de reformas del Código Penal del 2009)», en *La ley penal*, núm. 7442, julio de 2010; también Zugaldia Espinar, M., «Societas delinquere potest (Análisis de la reforma operada en el Código Penal español por la LO 5/2010, de 22 de junio)», *La Ley*, núm. 76, 2010, 5 ss.; Gómez-Jara Díez, C., «La responsabilidad penal de las personas jurídicas en la reforma del Código Penal», en *Diario La Ley*, núm. 7534, 2010.

(58) Sobre los criterios de imputación de la responsabilidad penal establecidos por el nuevo artículo 31-*bis* CP v. Morales Prats, F., en Quintero Olivares, G. (direc.), *La Reforma Penal de 2010*, cit., 47 ss.; Bacigalupo, S., «Los criterios de imputación de la responsabilidad penal de los entes colectivos y de sus órganos de gobierno» (art. 31-*bis* y 129 CP), en *Diario La Ley*, núm. 7541, 2011.

pabilidad propia del ente que, como en Italia (arts. 5 y 6 Dlgs. 231/2001), está basado en la comprobación de un déficit organizativo en virtud del cual se hace posible la comisión de un delito por parte de la persona física.

De manera análoga a lo que ha previsto el legislador italiano en el artículo 1, párrafo 3, del Dlgs. 8 de junio de 2001, núm. 231 (59), el artículo 31-*bis* CP se aplica solamente a las personas jurídicas privadas, con exclusión de las entidades de derecho público (Estado, Administraciones públicas territoriales e institucionales, Organismos Reguladores, Agencias y Entidades públicas Empresariales, organizaciones internacionales de derecho público), entidades estatales no económicas, o de aquellos privados que ejercen funciones públicas (por ejemplo organizaciones que ejercen potestades públicas o administrativas,), partidos políticos o sindicatos (art. 33-bis.5 CP).

El artículo 31-bis.2 CP establece, análogamente al artículo 8, párrafo 1, Dlgs. 8 de junio de 2001, núm. 231, que la responsabilidad penal de la persona jurídica es autónoma e independiente respecto a la de la persona física que ha cometido el delito. Por lo tanto, para que exista una responsabilidad penal del ente será suficiente probar que el representante o administrador de derecho o de hecho o un sujeto subordinado haya cometido un delito, también en el caso en que no se haya podido individualizar el concreto autor del hecho delictivo o no sea posible ejercer contra el mismo la acción penal (por ejemplo porque ha fallecido o no es imputable).

En conformidad al artículo 33-7 CP a la persona jurídica se le podrá aplicar una de las siguientes penas: a) disolución de la persona jurídica; b) suspensión de sus actividades por un plazo que no podrá exceder de cinco años; c) clausura de sus locales y establecimientos por un plazo que no podrá exceder de cinco años; d) prohibición de realizar en el futuro las actividades en cuyo ejercicio se haya cometido, favorecido o encubierto el delito; e) inhabilitación para obtener subvenciones y ayudas públicas, para contratar con el sector público y para gozar de beneficios e incentivos fiscales o de la Seguridad Social, por un plazo que no podrá exceder de quince años; f) intervención judicial para salvaguardar los derechos de los trabajadores o de los acreedores por el tiempo que se estime necesario, que no podrá exce-

(59) Artículo 1 Dlgs. núm. 231/2001: «1. Il presente decreto legislativo disciplina la responsabilità degli enti per gli illeciti amministrativi dipendenti da reato. 2. Le disposizioni in esso previste si applicano agli enti forniti di personalità giuridica e alle società e associazioni anche prive di personalità giuridica. 3. Non si applicano allo Stato, agli enti pubblici territoriali, agli altri enti pubblici non economici nonchè agli enti che svolgono funzioni di rilievo costituzionale».

der de cinco años. Alguna perplejidad provoca la falta de previsión en el catálogo de las penas de la publicación de la sentencia (60).

El artículo 33-*bis*.4 CP prevé un catálogo de circunstancias atenuantes de la responsabilidad penal de las personas jurídicas cuando hayan realizado, sucesivamente a la comisión de un delito y mediante su representante legal, una de las siguientes actividades: «a) haber procedido, antes de conocer que el procedimiento judicial se dirige contra ella, a confesar la infracción a las autoridades; b) haber colaborado en la investigación del hecho aportando pruebas, en cualquier momento del proceso, que fueran nuevas y decisivas para esclarecer las responsabilidades penales dimanantes de los hechos; c) haber procedido en cualquier momento del procedimiento y con anterioridad al juicio oral a reparar o disminuir el daño causado por el delito; d) haber establecido, antes del comienzo del juicio oral, medidas eficaces para prevenir y descubrir los delitos que en el futuro pudieran cometerse con los medios o bajo la cobertura de la persona jurídica».

De conformidad con lo que ha establecido el legislador italiano con los artículos 24 ss. D.lgs. núm. 231/2001, el legislador español ha limitado de momento la aplicación de la responsabilidad penal de las personas jurídicas a un *numerus clausus* de delitos (61). Entre ellos están previstos, en línea con el artículo 9 de la Decisión Marco 2005/222/JAH, también los nuevos delitos informáticos introducidos en el Código Penal con la reforma legislativa de 2010.

En base al artículo 197.3, párrafo 2, CP, cuando la persona jurídica es responsable de un delito de acceso no autorizado a datos y programas informáticos será sujeta a la pena de multa de seis a 2 años.

---

(60) Cfr. Zugaldia Espinar, M., *Societas delinquere potest*, cit., 14.

(61) Con la Ley Orgánica 05/2010 el legislador español ha introducido la responsabilidad penal de las personas jurídicas para los siguientes delitos: tráfico de órganos (art. 156-*bis* CP), trata de seres humanos (art. 177-*bis* CP), prostitución y corrupción de menores (art. 189-*bis* CP), acceso ilícito a datos y programas informáticos (art. 197.3 CP), estafa (art. 251-bis CP), insolvencias (art. 261-*bis* CP), daños informáticos (art. 264.4 CP), delitos relativos al mercado y consumidores y corrupción privada (art. 288 CP), receptación y otras conductas afines (art. 302.2 CP), delitos contra la Hacienda Pública y contra la Seguridad Social (art. 310-*bis* CP), delitos contra los derechos de los trabajadores (art. 318-bis.4 CP), delitos contra la ordenación del territorio (art. 319.4 CP), delitos contra el medio ambiente (arts. 327 y 328.6 CP), vertido de radiación ionizante (art. 343.3 CP), fabricación, manipulación, posesión y comercialización de explosivos (art. 348.3 CP), tráfico o favorecimiento del consumo de drogas tóxicas y estupefacientes (art. 369-*bis* CP), falsificación de tarjetas de crédito y débito y cheques de viaje (art. 399-*bis* CP), cohecho (art. 427.2 CP), tráfico de influencias (art. 430 CP), corrupción de funcionario público extranjero o de organización internacional (art. 445.2 CP), delitos de pertenencia a organización y grupos criminales (art. 570-*quater* CP) y financiación del terrorismo (art. 576-*bis*.3 CP).

Si la persona física que actúa en nombre o por cuenta o en el interés de una persona jurídica comete un delito de daño informático castigado con la pena de la reclusión superior a dos años, a la persona jurídica se le aplicará una multa del doble hasta el cuádruplo del perjuicio causado (art. 264.4, let. a) CP). En todos los demás casos se le aplicará a la persona jurídica una multa del doble al triple del perjuicio causado (art. 264.4, let. b), CP).

El loable objetivo de ejecutar las obligaciones internacionales en materia de responsabilidad de las personas jurídicas *(corporate liability)* ha sido conseguido solo parcialmente por parte del legislador español de 2010. La responsabilidad penal de las personas jurídicas no ha sido prevista por todos los delitos informáticos, como expresamente se establece en los artículos 12 y 13, párrafo 2, del Convenio del Consejo de Europa sobre el cibercrimen (62), puesto que concierne solamente aquellos delitos que han sido introducidos por la Ley Orgánica de 2010: es decir, para el acceso no autorizado a datos y programas informáticos (art. 197.3 CP) y los daños informáticos (art. 264, 1 y 2, CP).

En perspectiva de *lege ferenda*, será oportuno que el legislador español extienda la responsabilidad penal de las personas jurídicas también a los delitos de fraude informático (art. 248.2 CP), a las falsedades que se realizan a través de medios informáticos (arts. 390 ss. CP) y a los delitos relativos a la propiedad intelectual (arts. 270 ss. CP).

9. CONSIDERACIONES CONCLUSIVAS Y PERSPECTIVAS DE *LEGE FERENDA*

Haciendo un primer balance, si bien sumario, de la reforma legislativa de 2010, no faltan elementos críticos al lado de la comprensible supresión de las lagunas pre-existentes ya subrayadas por la mejor doctrina. Antes de todo la elección político-criminal del legislador español de castigar solamente el acceso ilícito a «datos y programas informáticos» (art. 197.3 CP) y no el mero acceso no autorizado a «sistemas informáticos», como previsto por el artículo 2 de la Decisión Marco 2005/222/JAH (esencialmente idéntico al art. 2 del Con-

(62) Sobre los criterios de atribución de la responsabilidad a las personas jurídicas previstos por el Convenio sobre el cibercrimen v. Silva Sánchez, J. M., «La responsabilidad penal de las personas jurídicas en el convenio del Consejo de Europa sobre cibercriminalidad», en Morales García, O. (dir.), *Delincuencia informática: problemas de responsabilidad, Cuadernos de derecho judicial*, núm. 9, 2002, 113 ss.

venio del Consejo de Europa sobre el cibercrimen) levanta algunas perplejidades. Si bien en la mayor parte de los casos a cada intrusión no autorizada en un sistema informático sigue la posibilidad de acceder a datos o a programas informáticos contenidos en ello, puede ocurrir que el criminal obtenga solamente el acceso al «sistema».

Piénsese por ejemplo en el *cracker* que se introduce en un sistema informático ajeno para instalar un programa espía (o *spyware),* que le permite tomar el control desde remoto del ordenador para utilizarlo con el fin de crear una *botnet*, para poner en circulación programas *malware*, para enviar *spam*, etc. Esta conducta, que representa una peligrosa amenaza para la integridad y la disponibilidad de los datos y de los sistemas informáticos, no sería penalmente relevante en base al nuevo artículo 197.3 CP, puesto que no implica necesariamente un acceso a datos informáticos contenidos en el sistema informático violado.

Fuertes dudas hace surgir, además, la autónoma previsión de la conducta omisiva de mantenerse en un sistema informático, cuya incriminación no está prevista en ninguna fuente internacional (63). Esta hipótesis, respecto a aquella actividad de acceso a datos y a programas informáticos, resulta ser de escasa ofensividad, haciendo lábil el límite del hecho penalmente relevante. La mera permanencia «abusiva» en un sistema informático genera el peligro que el sujeto agente pueda acceder a datos y a programas informáticos que están en el contenido, con el consiguiente peligro que pueda tomar conocimiento de ellos o modificar su contenido. De esta manera se sancionaría solamente el peligro indirecto para el bien jurídico de la confidencialidad y de la integridad de los datos, de los programas y de los sistemas informáticos (64).

---

(63) Han decidido sancionar, además de la conducta activa de acceso, también aquella omisiva de «mantenerse» en un sistema informático solo el legislador italiano (art. 615-*ter* CP), el frances (art. 323-1 *Code Penal:* «Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende») y belga (art. 550-*bis Code Penal:* «Celui qui, sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient, est puni d'un emprisonnement de trois mois à un an et d'une amende de vingt-six francs à vingt-cinq mille francs ou d'une de ces peines seulement»).

(64) Sobre la estructura de los delitos de peligro (eventual o necesariamente) indirecto y su conformidad a los fundamentales principios penalísticos de ofensividad y de proporcionalidad v. Dolcini, E., Marinucci, G., *Corso di diritto penale,* III, ed., Milano, 2001, 595. Sobre los problemas dogmáticos que presentan los delitos de peligro v., por todos, en la doctrina española Méndez Rodríguez, C., *Los delitos de peligro y sus técnicas de tipificación*, Madrid, 1993; Corcoy Bidasolo, M.., *Delitos de peligro y protección de bienes jurídico-penales supraindividuales*, Valencia, 1999;

En definitiva resulta ser criticable la elección de equiparar, desde un punto de vista sancionador, la conducta de acceso a datos y a programas informáticos a la de mantenerse en un sistema informático. Más correcta sería la incriminación, al lado del acceso «no autorizado», de aquél que se comete «excediendo los límites de la autorización», así como está por ejemplo previsto a nivel tanto federal cuanto estatal en los Estados Unidos de América (65), y más recientemente también en Bélgica, para castigar a aquellos empleados que acceden a todos o partes de los sistemas de la empresa fuera del ejercicio de sus funciones laborales (66).

En conformidad con la elección político-criminal de la Decisión Marco 2005/222/JAH, el legislador español de 2010 ha adoptado correctamente la bipartición entre daños de datos (art. 264.1 CP) y daños de sistemas informáticos (art. 264.2 CP). Sin embargo, el objetivo de ejecutar las obligaciones de fuentes europeas no ha sido plenamente conseguido.

En primer lugar, el legislador no ha considerado oportuno suprimir la referencia al ambiguo requisito de la «ajenidad» de los datos y programas informáticos y documentos electrónicos. Esta previsión representa una evidente anomalía, no solamente a la luz de las fuentes internacionales, sino también en el panorama jurídico europeo, en el que (a excepción de los arts. 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del Código Penal italiano), esta referencia ha sido omitida o sustituida con una más oportuna cláusula de ilicitud, expresada con las locuciones «sin derecho» o «sin autorización», que prescinde del derecho de «propiedad» y de la «posesión».

Mendoza Buergo, B., *Límites dogmáticos y político-criminales de los delitos de peligro abstracto*, Granada, 2001; ID., «La configuración del injusto (objetivo) de los delitos de peligro abstracto», en *RDPCr,* núm. 9, 2002, 39 ss.; en la doctrina italiana v. Gallo, E., *Riflessioni sui reati di pericolo*, Padova, 1970; Fiandaca, G., «La tipizzazione del pericolo», en *Dei delitti e delle pene*, 1984, 441 ss.; Angioni, F., *Il pericolo concreto come elemento della fattispecie penale: struttura oggettiva*, Milano, 1994; Parodi Giusino, M., *I reati di pericolo tra dogmatica e politica criminale*, Milano, 1990; Canestrari, S., voce «Reati di pericolo», en *Enciclopedia Giuridica Treccani*, vol. XXIV, 1991, 1 ss.

(65) En base a la definición del § 1030 (I)(6) U.S.C. acceder a un sistema informático excediendo los límites de la autorización significa: «access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter». En extenso v. Salvadori, I., *L'esperienza giuridica*, cit.

(66) Artículo 550-*bis*, para. 2, *Code Pénal:* «Celui qui, avec une intention frauduleuse ou dans le but de nuire, outrepasse son pouvoir d'accès à un système informatique, est puni d'un emprisonnement de six mois à deux ans et d'une amende de vingt-six francs à vingt-cinq mille francs ou d une de ces peines seulement».

Fuertes perplejidades surgen además con referencia a la posibilidad de subsumir en los tipos delictivos de los artículos 264.1 e 264.2 CP los daños físicos, cometidos contra las partes *hardware* de un sistema informático o telemático, que no afectan a las partes lógicas. Si estos daños pudieran ser reconducidos al delito tradicional de daño en la propiedad ajena (art. 263 CP), que prevé un tratamiento sancionador más severo, estaríamos frente a una evidente disparidad de tratamiento entre hechos que lesionan el análogo bien jurídico de la integridad y disponibilidad de sistemas informáticos. Sería por lo tanto oportuno que el legislador español introdujera un sub-tipo autónomo dentro del artículo 264 CP, para castigar expresamente los daños «físicos» de sistemas informáticos, así como establece por ejemplo el § 303b, par. 1, núm. 3 del Código Penal alemán (StGB) (67).

En el adecuar la propia legislación penal en materia de criminalidad informática a las obligaciones internacionales el legislador español, a diferencia de lo que han hecho la mayoría de los legisladores de los Países europeos (Alemania, Italia, Francia, Austria, Romania, Portugal, etc.) (68), ha dado actuación solamente a las disposiciones de la Decisión Marco 2005/222/JAH. De esta manera el legislador español ha perdido la ocasión para dar plena ejecución a las demás importantes disposiciones del Convenio del Consejo de Europa sobre el cibercrimen, que representa hoy en día el instrumento supranacional más importante en la lucha contra la criminalidad informática y que España ha firmado ya desde el 23 de noviembre de 2001, sin proceder luego a su sucesiva ratificación (69). Solamente con la reciente decisión del

---

(67) § 303b.1, n.3 StGB: «eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft».

(68) V. Picotti, L., Salvadori, I., *National legislation implementing the Convention on cybercrime: comparative analysis and good practices,* August 2008, disponible a la siguiente página web http://www.coe.int/t/dghl/ cooperation/ economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp. Para un análisis de la Ley de 18 de marzo de 2008, núm. 48, con la cual el legislador italiano ha ratificado y dado ejecución en el ordenamiento interno a las prescripciones del Convenio del Consejo de Europa sobre el cibercrimen v. Picotti, L., «Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo», en *Diritto dell'Internet,* núm. 5, 2008, 437 ss.

(69) El listado de los treinta países que al día de hoy han ratificado el Convenio sobre el cibercrimen está disponible en el portal del Consejo de Europa a la siguiente pagina web http://conventions.coe.int/Treaty/ Commun/ChercheSig.asp?NT=185&CM=8&DF= &CL= ENG. Sobre la importancia del Convenio del Consejo de Europa sobre el cibercrimen v. en doctrina Gercke, M., «The Slow Wake of a Global Approach Against Cybercrime», in *CRI,* núm. 5, 2006, 144; Sieber, U., «Mastering complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law», en Delmas-Marty, M., Pieth, M., Sieber, U. (eds.), *Les*

Parlamento español del pasado día 3 de junio de 2010, ha sido formalmente ratificado el Convenio del Consejo de Europa, sin que luego haya seguido su efectiva actuación en el ordenamiento interno, ni con referencia a las disposiciones en materia de derecho penal sustancial, ni con referencia a aquellas en materia procesal (70).

A pesar de las relevantes novedades en la lucha contra la delincuencia informática introducidas por la Ley Orgánica 05/2010, destaca el Código Penal español la falta de una norma directa a castigar, en línea con el artículo 3 del Convenio del Consejo de Europa sobre el cibercrimen (CoC) (71), las conductas de interceptación de datos informáticos (o *data interference),* que pueden ser subsumidas solo parcialmente en los artículos 197.1, 197.2 y 278.1 CP. También criticable es la falta de previsión de una norma específica para castigar, como lo requiere el artículo 6 CoC, el abuso de los dispositivos (o *misuse of devices)* (72), es decir, la producción, la posesión, la venta,

---

chemins de l'Harmonisation Pènale. Harmonising Criminal Law, Collection de L'UMR de Droit Comparè de Paris, Bd. 15. Paris, Sociètè de lègislation comparèe, 2008, 127 ss.,141. Cfr. también el informe explicativo de la Decisión Marco 2005/222/JAH, que define el Convenio del Consejo de Europa como la iniciativa legislativa más avanzada a nivel internacional en la lucha contra la ciberdelincuencia (COM (2002) 173 FINAL., OL 203/E 27.8.2002, 109-113, núm. 27).

(70) El instrumento de ratificación del Convenio sobre el cibercrimen, publicado en el *Boletín Oficial del Estado*, núm. 226/2010 está disponible en la siguiente página web http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

(71) Artículo 3 CoC: «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system».

(72) Artículo. 6 CoC: «1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5

la importación, la distribución, la puesta a disposición de un dispositivo, programa informático, código de acceso o palabra clave con la finalidad de cometer un delito contra la confidencialidad, la disponibilidad o la integridad de datos o sistemas informáticos, y además las falsedades informáticas *(computer-related forgery)* (73).

Sin embargo, aun más criticable es la falta de actuación de las fundamentales disposiciones procesales en materia de cooperación judiciaria establecidas por el Convenio del Consejo de Europa sobre cibercrimen. En la falta de normas *ad hoc* en materia de orden de presentación (art. 18 CoC), registro y confiscación de datos informáticos almacenados (art. 19 CoC), interceptación y obtención en tiempo real de datos relativos al contenido y al tráfico (arts. 20 y 21 CoC), será difícil si no imposible por las autoridades españolas de *law enforcement* poder proceder a realizar investigaciones en materia de criminalidad informática y además proporcionar efectiva asistencia a las autoridades de otros países.

Por lo tanto es deseable que el legislador español se active para dar efectiva actuación también a las disposiciones del Convenio del Consejo de Europa sobre el cibercrimen. Solamente de esta manera podrá conseguir el encomiable objetivo, perseguido por la Ley Orgánica 05/2010, de armonizar la propia legislación penal en materia a las indicaciones de fuente internacional, presupuesto este esencial para contrastar de manera eficaz la criminalidad informática.

---

of this Convention, such as for the authorised testing or protection of a computer system». 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article».

(73) «Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches».