LOS DELITOS CONTRA LA CONFIDENCIALIDAD, LA DISPONIBILIDAD Y LA INTEGRIDAD DE LOS DATOS Y SISTEMAS INFORMÁTICOS
Regulación Española*

Iván Salvadori

Resumen

En el presente trabajo se analizan 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 otorga 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). Finalmente, para concluir, se desarrollan en perspectiva comparada algunas consideraciones críticas sobre la formulación de estos nuevos delitos informáticos.

Palabras clave: Derecho penal informático – Ley Orgánica 5/2010 - cibercrimen – intrusismo informático - daños informáticos – Convenio sobre Cibercrimen.

El autor: Doctor europeo en Derecho penal económico y Derecho penal informático por la Universidad de Verona (Italia); Profesor de Derecho Penal y Derecho Penal Informático en la Universidad de Barcelona (España). <ivansalvadori@gmail.com>

* Artículo evaluado.

CRIMES AGAINST CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF DATA AND INFORMATION SYSTEMS. The Spanish Normativity

Abstract

The present work analizes the current normativity protecting confidenciality, integrity, and availability of data and information systems, which have been introduced in the Spanish Criminal Code by Law 5/2010 of June 22nd, by amending the Law 10/1995 of November 23rd. In this respect, special attention is given to the new offenses of illegal access to computer data and programs (art. 197.3 CP) and data or computer system corruption crimes (Art. 264.1 and Art. 264.2 CP). Finally, some critical considerations on the formulation of these new crimes are presented from a comparative perspective.

Key words: Computer Criminal Law, Law 5/2010, Cybercrime, Computer intrusion, Computer damage, Convention on Cybercrime.

The author: PhD in Criminal Law and Computer Crime Law graduate of the *University of Verona* (Italy); professor of Criminal Law and Computer Crime Law at the *University of Barcelona* (Spain).

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[2]. El objetivo principal de la reforma, que en parte retomó el Anteproyecto de Ley Orgánica de 2008[3], fue dar ejecución a las obligaciones internacionales y colmar las lagunas de punibilidad surgidas en la práctica, que por lo 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 muchos delitos del Código Penal, entre ellos los relativos a la explotación de menores, a la trata de seres humanos, 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 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[4].

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[5].

---

2 CONGRESO DE DIPUTADOS. *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 pagina 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 ALVAREZ GARCÍA F.J., GONZÁLEZ CUSSAC J.L. (dirs.), *Consideraciones a propósito del proyecto de Ley de 2009 de modificación del Código penal*, Valencia, 2010.

3 CONGRESO DE DIPUTADOS. *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 NUÑEZ 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*, n. 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.

4 CONGRESO DE DIPUTADOS. *Proyecto de Ley Orgánica*, cit., *Preámbulo*, XIV.

5 Por un primer comentario sistemático a la Ley Orgánica 5/2010 v. ALVAREZ 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 Comentarios*, Navarra, 2010. Sobre el contexto político-criminal de la Ley orgánica 05/2010 v. SILVA SANCHEZ J.M., *La reforma del Código Penal: una aproximación desde el contexto*, en *Diario La Ley*, nº 7464, 9 Sep. 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*)[6] introducidos por la mencionada Ley Orgánica 5/2010, sin tomar en consideración aquellos que pueden ser cometidos también a través de las redes informáticas (como por ejemplo el delito de "*child-grooming*" o "ciber-acoso", del art. 183-*bis* CP[7], el de utilización ilícita de tarjetas de crédito del art. 248.2, let. c), CP, etc.)[8]. 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 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 2 y 4). El análisis de la normativa penal anterior a la reforma permitirá evaluar si con la Ley Orgánica 5/2010 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 3) y a los delitos de daños de datos (párrafo 5) y de sistemas informáticos (párrafo 6). Finalmente, para concluir, se desarrollaran algunas consideraciones críticas sobre la formulación de los nuevos delitos informáticos introducidos en el Código Penal español por la Ley Orgánica 5/2010 (párrafo 7).

---

6 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 protegèes et techniques de formulation des infractions en droit pènal de l'informatique*, in *Revue International de Droit Pènal*, vol. 77, 2006, 533.

7 CONGRESO DE DIPUTADOS. Art. 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 una primera análisis del art. 183-*bis* CP v. VIVES ANTON T.S., ORTS BERENGUER E., CARBONELL MATEU J.C., GONZALEZ CUSSAC J.L., MARTINES-BUJAN PEREZ C., *Derecho penal, Parte especial*, III ed., Valencia, 2010, 269-271. Para un análisis del delito de *child-grooming* en perspectiva comparada v. SALVADORI I., *Possesso di pornografia infantile, accesso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale*, en RUGGIERI F., PICOTTI L.(coord.), *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*, Torino, 2011, 26 ss.

8 CONGRESO DE DIPUTADOS. Art. 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* ».

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*)[9].

En 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[10]. Paradigmático era el art. 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[11]. De igual manera se afirmó en referencia a los delitos de daños "lógicos" (art. 264.1 CP), que en ellos podían ser subsumidas las conductas de acceso no autorizado instrumentales a la agresión de datos y programas informáticos[12]. Por tanto, el simple acceso ilícito a un sistema informático hubiera sido ya penado en el ordenamiento jurídico español, en cuanto constituya una tentativa de cometer una violación de la intimidad o un daño informático[13].

---

9 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.; MORON LERMA E., *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red,* Pamplona, 2002, 55 ss.; GONZÁLEZ RUS J.J., *Daños a través de Internet*, en AA.VV., *Homenaje al Prof. Dr. G.R. Mourullo*, Navarra, 2005, 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 MARTIN M.A., *Los ataques contra los sistemas informáticos: conducta de hacking. Cuestiones políticos criminales*, en *Sistema penal*, n.1, 2008, 74. En la jurisprudencia v. AP Tarragona, 23 julio 2001, JUR 310139/01.

10 En este sentido v. GONZÁLEZ RUS J.J., *El cracking y otros supuestos de sabotaje informático*, en *Estudios jurídicos, Ministerio Fiscal,* n. 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. MORON LERMA E., *Internet y Derecho penal*, cit., 55.

11 Cfr. MORON LERMA E., *Internet y Derecho penal*, cit., 58-64.

12 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.

13 En este sentido v. GONZÁLEZ RUS J.J., *Daños a través de Internet*, cit., 1482.

Mayores dudas han surgido en doctrina y en jurisprudencia en referencia a la posibilidad de castigar, en falta de una disposición especifica, las conductas de simple acceso ilícito a un sistema informático realizadas sin finalidad ilícita ulterior (el llamado "*hacking blanco*")[14]. 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)[15].

El articulo 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.)[16].

La conducta típica del art. 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[17].

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.

[14] 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* n.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.

[15] Cfr. MORON LERMA E., *Internet y Derecho penal*, cit., 55-58; GONZÁLEZ RUS J.J., *Art. 256 CP*, en COBO DEL ROSAL M. (coord.), *Comentarios al Código penal*, Tomo VIII, Madrid, 2004, 555.

[16] En doctrina v. ORTS BERENGUER E., ROIG TORRES M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia, 2001; SALVADORI I., *Delincuencia informática*, en CORCOY BIDASOLO M. (dir.), *Derecho Penal, Parte especial*, tomo I, Valencia, 2011, 497.

[17] En este sentido 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, 771.

Paradigmáticas 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[18].

Teniendo en consideración la ubicación sistemática y la formulación de la norma, la doctrina mayoritaria ha afirmado que el bien jurídico protegido por el art. 256 CP es el patrimonio[19]. Sin embargo, el carácter patrimonial del interés protegido por la norma impide subsumir en el art. 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 legitimo titular del sistema informático[20]. 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[21].

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 de 2010 ha introducido en el Código Penal una disposición *ad hoc* para sancionar el acceso no autorizado a datos y programas informáticos (o *intrusismo informático*).

---

18 Cfr. MORON 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., *Art. 256 CP*, cit., 553.

19 V., por todos, ORTS BERENGUER E., ROIG TORRES M., *Delitos informáticos,* cit., 76; MORON LERMA E., *Internet y Derecho penal*, cit., 56.

20 Cfr. MORON LERMA E., *Internet y Derecho penal*, cit., 56; análogamente GUTIÉRREZ FRANCÉS M.L., *El intrusismo informático*, cit., 1174 ss.

21 En este sentido v. GUTIÉRREZ FRANCÉS M.L., *El intrusismo informático* (hacking) ¿Represión penal autónoma?, en Informática y Derecho, n. 12-15, 1996, 1175; MORON LERMA E., *Internet y Derecho penal,* cit., 57.

El nuevo párrafo tercero del art. 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)[22]. Muy similares son también las conductas típicas. El art. 197.3 CP, de manera análoga al art. 615-*ter* del Código Penal italiano[23], 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 art. 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 de 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[24].

---

22 CONGRESO DE DIPUTADOS. Art. 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*».

23 CONGRESO DE DIPUTADOS. Art. 615-*ter*, comma 1, c.p. (« 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* ». Para un análisis de la norma italiana v. SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, en PICOTTI L. (coord.), *Tutela penale della persona e nuove tecnologie. Quaderni per la riforma del codice penale*, Padova, 2012 (en prensa); ID, *Cuando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite delimitano l'ambito di applicazione dell'art. 615-ter c.p.*, en *Riv. trim. dir. pen,. econ.*, 2012 (en prensa).

24 Sobre la interpretación de la conducta de "acceso" a un sistema informatico v. SALVADORI I., *L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking*, en *Riv. it. dir. proc. pen.*, n.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 art. 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 esta 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[25]. 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[26]. 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 art. 197.3 CP castiga la conducta omisiva del «mantenerse» en un sistema contra la voluntad del legítimo titular[27]. El objetivo de esta previsión, que

[25] Diferente ha sido la elección del legislador rumano, que yendo más allá del art. 1 del Convenio sobre el cibercrimen, en el art. 35, let. h), de la ley 21 de Abril de 2003, n. 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».

[26] Análogamente v., en la doctrina alemana HILGENDORF E., *§ 202a StGB*, *Leipziger Kommentar*, 2010, 1448-1449, Rdn. 34; KARGL W., *§ 202a StGB*, en KINDHÄUSER U., NEUMANN U., PAEFFGEN H.-U. (Hrsg.), *Strafgesetzbuch, Nomoskommentar*, Band 2, 3. Auf., 2010, 486.

[27] Con referencia a la análoga hipótesis del "mantenerse" en un sistema informático, prevista por el art. 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 n. 547*, en *Legisl. Pen.*, 1996, 100; PICOTTI L., *voce Reati informatici,* en *Enciclopedia 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.

está contemplada también en el Código Penal italiano (art. 615-*ter* c.p.), parece castigar aquellas hipótesis muy frecuentes en la práctica en las que, después de una inicial introducción obtenida de manera legitima o casual, el sujeto agente se "mantiene" en el sistema ajeno contra la voluntad de quién 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 legitimo 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 de 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 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[28].

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 trabajo, 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.

[28] En este sentido v. también CARRASCO ANDRINO M., *El delito de acceso ilícito a los sistemas informáticos*, en ALVAREZ GARCÍA F.J., GONZÁLEZ CUSSAC J.J. (dir.), *Comentarios*, cit., 254.

Por la formulación del art. 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 "*jus excludendi alios*") de disponer de sus datos y programas informáticos, independientemente de su contenido (secreto o reservado) o de su valor económico[29] e indirectamente el interés jurídico a la seguridad informática[30].

[29] 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,* n. 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. En sentido similar v. también SALVADORI I., *L'esperienza giuridica*, cit., 1281; ID., *La fattispecie di accesso abusivo*, cit.

[30] Sobre el nuevo bien jurídico de la seguridad informática v. PICOTTI L., *Sistematica dei reati informatici*, in ID. (coord.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 74; SALVADORI I., *L'accesso abusivo a un sistema informatico*, cit.

Conforme a lo establecido en el art. 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 art. 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 art. 570-*bis* CP, introducido por la Ley Orgánica 5/2010, 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*»[31].

Por su parte, el nuevo art. 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*»[32].

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 especifico: el "sabotaje informático"[33].

El art. 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 documentos electrónicos ajenos contenidos en redes, suportes 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

[31] Sobre el concepto legal de organización criminal v. GARCÍA RIVAS N., LAMARCA PÉREZ C., *Organizaciones y grupos criminales*, en ALVAREZ GARCIA F.J., GONZALEZ CUSSAC J.J. (direc.), *Comentarios*, cit., 507-508.

[32] Sobre el concepto legal de grupo criminal v. GARCÍA RIVAS N., LAMARCA PÉREZ C., *Organizaciones y grupos criminales*, in ALVAREZ GARCIA F.J., GONZALEZ CUSSAC J.J. (direc.), *Comentarios*, cit., 510-512.

[33] Sobre las tentativas jurisprudenciales y doctrinales de reconducir en la 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.

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[34].

Un sector de la doctrina había considerado inútil y prescindible la introducción en el Código Penal de 1995 del art. 264.2 CP, dado que estimaba que las conductas de daños "lógicos" habrían podido ser pacíficamente reconducidas en el delito común de daños[35]. Este último, -señalaba este sector- contrariamente, por ejemplo al tipo delictivo de daños previsto por el art. 635 del Código penal italiano[36], no requería expresamente un daño a una "cosa" material, sino a la "propiedad" ajena[37]. 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[38].

El hecho típico del art. 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 "físicos" cometidos contra suportes materiales que contenían los mencionados "objetos" informáticos[39]. 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 « *atos, programas o documentos informáticos*»[40]. En particular la conducta violenta de daños tenía que recaer sobre datos, documentos

---

[34] 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.

[35] GONZÁLEZ RUS J.J., *Aproximación al tratamiento penal*, cit.

[36] Art. 635, comma 1, c.p. ("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* ».

[37] 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,* in *Cuadernos de Derecho Judicial,* Madrid, 1996, 295.

[38] GONZÁLEZ RUS J.J., *Aproximación al tratamiento penal,* cit., 138-142.

[39] Cfr. ORTS BERENGUER E., ROIG TORRES M., *Delitos informáticos*, cit., 79.

[40] Sobre la definición de los objetos materiales típicos del art. 264.2 CP v. GONZÁLEZ RUS J.J., *Daños a través de Internet*, cit., 1473 ss.

y programas informáticos contenidos en un soporte físico (por ej. CD, DVD, tarjetas magnéticas, etc.), archivados o almacenados en un sistema informáticos o en fase de transmisión en red (por ej. a través de Internet, WI-FI, etc.).

El legislador 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[41]. 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 legitimo interés a su integridad y disponibilidad, pese a no ser propietarios en sentido civilístico.

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 art. 264.2 CP, que no permitían sancionar las siempre más peligrosas formas de ataques a los sistemas informáticos que se cometen a través de Internet (por ej. ataques *Denial of service, Netrike*, *Spamming*, etc.)[42], 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 art. 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,*

[41] 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*, in *Eguzkilore: Cuaderno del Instituto Vasco de Criminología*, n. 21, 2007, 17 Análogamente v. en la doctrina italiana, con referencia al hoy abrogado art. 635-*bis* c.p. introducido por la Ley n. 547/1993 y modificado por la Ley n. 48/2008, 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.

[42] 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*, n.3, 2008, 329 ss.

suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave».

Respecto al hoy derogado art. 264.2 CP, el legislador de 2010 ha previsto en el hecho típico del nuevo art. 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[43]. 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.)[44].

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 modificación del nombre del archivo en el que son contenidos aquellos o por medio de la sustracción del soporte en el que están archivados[45].

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

---

43 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.

44 En este sentido v. en la jurisprudencia italiana Cass., sez. V, 18 novembre 2011 (dep. 5 marzo 2012), n. 8555, disponible en www.pemale.it.

45 Afirma que estas conductas no pueden ser subsumidas en el tipo delictivo de daño del art. 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.

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 art. 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[46]. La previsión de esta locución indeterminada produce fuertes perplejidades con referencia al respeto del fundamental principio de taxatividad.

De forma totalmente pleonástica, el art. 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 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 art. 264.2 CP, introducido en el Código Penal del 1995, es el objeto material del nuevo tipo delictivo de daños de datos informáticos del art. 264.1 CP. Completamente redundante es la previsión junto a los datos y a los programas

[46] 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.

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 art. 7, párrafo 1 y 2, de la Decisión Marco 2005/222/JAI, la Ley Orgánica 5/2010 introduce un nuevo párrafo al art. 264 CP, para castigar de manera agravada los daños cometidos en el marco de una organización criminal (art. 264.3, n. 1, CP), y el supuesto en que se produzcan «daños de especial gravedad» o que afecten «intereses generales»[47].

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 art. 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 modifique la formulación del tipo delictivo o ofrezca criterios para definir de manera más precisa esta locución indeterminada.

Al mismo tiempo, imprecisa resulta ser la formulación del art. 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 correcto funcionamiento depende cada vez mas 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 individuado, de conformidad con las indicaciones de

[47] CONGRESO DE DIPUTADOS. Art. 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*».

fuente internacional[48], como el interés del legítimo titular a la plena disponibilidad e integridad de los datos y de los programas informáticos[49].

El nuevo delito de daños de sabotaje informático (art. 264.2 CP)

Con el objetivo de ejecutar la obligación de incriminar las conductas de «*system interference*», requerida por el art. 3 de la Decisión Marco 2005/222/JAH, el legislador de 2010 ha introducido un nuevo párrafo segundo en el art. 264 CP. El nuevo delito de daño de sistemas informáticos (o "sabotaje informático") 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 art. 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 art. 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, sino también a las de muchos ordenamientos jurídico-penales europeos (véase por ejemplo el § 303b del Código Penal alemán[50], el art. 635-*quater*

[48] 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.

[49] En este sentido v. ya CORCOY BIDASOLO M., *Protección penal*, cit.; más reciente támbien SALVADORI I., *Delincuencia informática*, cit., 491. En contra, GONZÁLEZ RUS J.J., *Naturaleza y ámbito de aplicación*, cit., 1293, 1294, según el cual el bien jurídico tutelado tiene que ser individuado como la propiedad del titular de los datos dañados.

[50] § 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*».

del Código Penal italiano[51], etc.) permite de 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 (*Spam*), cuyo efecto es interferir de manera grave en el correcto funcionamiento de un sistema de información[52].

Comprensible es la elección del legislador 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 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 art. 3 de la Decisión Marco 2005/222/JAH, el resultado típico del art. 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 art. 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, DDoS* o *Mail-Bombing*).

Algunas dudas surgen sobre la posibilidad de reconducir al art. 264.2 CP los daños informáticos "físicos", es decir, aquellos daños cometidos a través de ataques a la parte *hardware* de un sistema 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 art. 264.2 CP, pero solamente si causan de manera indirecta un daño a datos y

---

51 Art. 635-*quater* c.p. (*"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*». Para una análisis de la norma italiana v. SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, en *Riv. it. dir. proc. pen.*, n.1/2012 (en prensa).

52 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.

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 art. 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 5).

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 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 art. 2 de la Decisión Marco 2005/222/JAH (esencialmente idéntico al art. 2 del Convenio 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 de 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 bas al nuevo art. 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 del mantenerse en un sistema informático, cuya incriminación no está prevista en ninguna fuente internacional[53]. 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 modificarlos. 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[54].

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 del 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[55], y más recientemente también en Bélgica, para castigar aquellos empleados que acceden a todos o partes de los sistemas de la empresa fuera del ejercicio de sus funciones laborales[56].

---

53 Han decidido sancionar, además de la conducta activa de acceso, también aquella omisiva del "mantenerse" en un sistema informático solo el legislador italiano (art. 615-*ter* c.p.), 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*»).

54 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; MENDOZA BUERGO B., *Limites 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,* n.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.

55 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.; ID, *Cuando un* insider *accede abusivamente ad un sistema informatico*, cit.

56 Art. 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*».

En conformidad con la elección político-criminal de la Decisión Marco 2005/222/JAH, el legislador de 2010 ha correctamente adoptado 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-*quarter* e 635-*quinquies* del Código Penal italiano)[57], 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".

Fuertes perplejidades surgen además con referencia a la posibilidad de subsumir en los tipos delictivos de los arts. 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 (*software*). 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. Seria por lo tanto oportuno que el legislador español introdujera un sub-tipo autónomo dentro del art. 264 CP, para castigar expresamente los daños "físicos" de sistemas informáticos, así como establece por ejemplo el § 303b, par. 1, n.3 del Código Penal alemán (StGB)[58].

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.)[59], ha dado actuación solamente a las

57 SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici*, cit.

58 § 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*» .

59 V. PICOTTI L., SALVADORI I., *National legislation implementing the Convention on cybercrime: comparative analysis and good practices,* August 2008, disponible a la siguiente pagina web http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-presentations/default en.asp. Para un analísis de la Ley de 18 de marzo de 2008, n. 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*, n. 5, 2008, 437 ss.

disposiciones de la Decisión Marco 2005/222/JAH. De esta manera el legislador de 2010 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 mas importante en la lucha a la criminalidad informática y que España ha firmado ya desde el 23 de noviembre 2001, sin proceder luego a su sucesiva ratificación[60]. Solamente con la decisión del Parlamento español del 3 de junio 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[61].

A pesar de las relevantes novedades en la lucha a la delincuencia informática introducidas con la Ley Orgánica 5/2010, destaca el Código Penal español la falta de una norma directa a castigar, en línea con el art. 6 del Convenio del Consejo de Europa sobre el cibercrimen (CoC) el abuso de dispositivos («*misuse of devices*»)[62], es decir, la producción, la posesión, la venta, la importación, la distribución, la

[60] 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*, en *CRI*, n. 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 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 mas avanzada a nivel internacional en la lucha a la ciberdelincuencia (COM (2002) 173 FINAL., OL 203/E 27.8.2002, 109-113, n. 27).

[61] El instrumento de ratifica del Convenio sobre el cibercrimen, publicado en el *Boletín Oficial del Estado*, n. 226/2010 es disponible en la siguiente pagina web http://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

[62] Art. 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 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*».

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, en línea con el art. 7 CoC, las falsedades informáticas («*computer-related forgery*»)[63]. 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 trafico (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 5/2010, 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.

Referencias bibliográficas

ALVAREZ GARCÍA F.J., GONZÁLEZ CUSSAC J.L. (dirs.), *Consideraciones a propósito del proyecto de Ley de 2009 de modificación del Código penal*, Valencia, 2010.

ANGIONI F., *Il pericolo concreto come elemento della fattispecie penale: struttura oggettiva*, Milano, 1994.

CANESTRARI S., Voce *Reati di pericolo*, en *Enciclopedia Giuridica Treccani*, vol. XXIV, 1991, 1 ss.

CASANUEVA SANZ I., PUEYO RODERO J.A. (coord.), *El Anteproyecto de modificación del Código Penal de 2008: algunos aspectos*, Bilbao, 2009.

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.

[63] Art. 7 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 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*».

COBO DEL ROSAL M. (coord.), *Comentarios al Código penal*, Tomo VIII, Madrid, 2004.

CORCOY BIDASOLO M., *Protección penal del sabotaje informático. Especial consideración de los delitos de daños*, en *Revista Jurídica La Ley*, n.1/1990, 1000 ss.

CORCOY BIDASOLO M., *Delitos de peligro y protección de bienes jurídico-penales supraindividuales*, Valencia, 1999.

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.

DOLCINI E., MARINUCCI G., *Corso di diritto penale*, III ed., Milano, 2001.

FIANDACA G., *La tipizzazione del pericolo*, en *Dei delitti e delle pene*, 1984, 446 ss.

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,* n. 24/2009, 3 ss.

GALLO E., *Riflessioni sui reati di pericolo*, Padova, 1970.

GERCKE M., The Slow Wake of a Global Approach Against Cybercrime, en CRI, n. 5, 2006, 140 ss.

GERCKE M., *Die Cybercrime Konvention,* en *Computer und Recht International,* 2004, 782 ss.

GONZÁLEZ RUS J.J., *Daños a través de Internet*, en AA.VV., *Homenaje al Prof. Dr. G.R. Mourullo*, Navarra, 2005, 1469 ss.

GONZÁLEZ RUS J.J., *El cracking y otros supuestos de sabotaje informático*, en *Estudios jurídicos, Ministerio Fiscal,* n. 2, 2003, 246 ss.

GONZÁLEZ RUS J.J., *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, 1281 ss.

GUTIÉRREZ FRANCÉS M.L., *El intrusismo informático* (hacking) *¿Represión penal autónoma?*, en *Informática y Derecho*, n. 12-15, 1996, 1163 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, Cuadernos de Derecho Judicial,* Madrid, 1996, 250 ss.

HILGENDORF E., FRANK T., VALERIUS B., *Computer und Internetstrafrecht*, Berlin, Heidelberg, 2005.

HOEREN T., SIEBER U. (Hrsg.), *Handbuch Multimedia- Recht*, München, 2009

KINDHÄUSER U., NEUMANN U., PAEFFGEN H.-U. (Hrsg.), *Strafgesetzbuch, Nomoskommentar*, Band 2, 3. Auf., 2010.

MANTOVANI F., *Danneggiamento di sistemi informatici e telematici,* en *Dig. disc. pen., vol.* agg., Torino, 2004.

MENDOZA BUERGO B., *Limites dogmáticos y político-criminales de los delitos de peligro abstracto*, Granada, 2001.

MORON LERMA E., *Internet y derecho penal: Hacking y otras conductas ilícitas en la Red,* Pamplona, 2002.

MUCCIARELLI F., *Commento agli art. 1,2,4 e 10 l. 1993 n. 547*, en *Legisl. Pen.*, 1996, 100 ss.

MUÑOZ CONDE F., *Derecho Penal, Parte Especial*, XVIII ed., Valencia, 2010.

ORTÍZ DE URBINA GIMENO I. (coord.), *Memento Experto Reforma penal,* Madrid, 2010.

ORTS BERENGUER E., ROIG TORRES M., *Delitos informáticos y delitos comunes cometidos a través de la informática,* Valencia, 2001.

PARODI GIUSINO M., *I reati di pericolo tra dogmatica e politica criminale*, Milano, 1990.

PECORELLA C., *Il diritto penale dell'informatica*, II ed. amp., Padova, 2006.

PICA G., *Diritto penale delle tecnologie informatiche,* Torino, 1999.

PICOTTI L., *Biens juridiques protegèes et techniques de formulation des infractions en droit pènal de l'informatique*, in *Revue International de Droit Pènal*, vol. 77, 2006, 525 ss.

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

PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, en *Diritto dell'Internet*, n. 5, 2008, 437 ss.

PICOTTI L., SALVADORI I., *National legislation implementing the Convention on cybercrime: comparative analysis and good practices,* August 2008, en http://www.coe.int/t/dghl/ co-operation/economiccrime/cybercrime/Documents/Reports-Presentations/default_en.asp

PICOTTI L., *voce Reati informatici,* en *Enciclopedia Giuridica Treccani, Aggiorn.,* Roma, 2000, 1 ss.

QUINTERO OLIVARES G. (dir.), *La reforma Penal de 2010: Análisis y Comentarios*, Navarra, 2010.

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.

ROMEO CASABONA C.M. (coord.), *El cibercrimen. Nuevos retos jurídico-penales, nuevas respuestas político-criminales*, Granada, 2006.

RUEDA MARTÍN M.A., *Los ataques contra los sistemas informáticos: conducta de hacking. Cuestiones políticos criminales*, en *Sistema penal*, n.1, 2008, 157 ss.

SALVADORI I., *Delincuencia informática*, en CORCOY BIDASOLO M. (dir.), *Derecho Penal, Parte especial*, tomo I, Valencia, 2011, 485 ss.

SALVADORI I., *Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante*, en *Riv. It. Dir. Proc. Pen.*, n.1/2012 (en prensa).

SALVADORI I., *L'esperienza giuridica degli Stati Uniti d'America in materia di hacking e cracking*, en *Riv. it. dir. proc. pen.*, n.3/2008, 1243 ss.

SALVADORI I., *L'accesso abusivo ad un sistema informatico o telematico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, en PICOTTI

L. (coord.), T*utela penale della persona e nuove tecnologie. Quaderni per la riforma del codice penale*, Padova, 2012 (en prensa).

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*, n.3, 2008, 329 ss.

SALVADORI I., *Cuando un* insider *accede abusivamente ad un sistema informatico o telematico*, en *Riv. trim. dir. pen. econ.*, n.1, 2012 (en prensa).

SALVADORI I., *Possesso di pornografia infantile, accesso a siti pedopornografici, child-grooming e tecniche di anticipazione della tutela penale*, en RUGGIERI F., PICOTTI L. (coord.), *Nuove tendenze della giustizia penale di fronte alla criminalitá informatica. Aspetti sostanziali e processuali*, Torino, 2011, 20 ss.

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 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.

SIEBER U., *Organised crime in Europe: the threat of cybercrime*, Council of Europe, Strasbourg, 2005.

SILVA SÁNCHEZ J.M., *La reforma del Código Penal: una aproximación desde el contexto*, en *Diario La Ley*, nº 7464, 9 Sep. 2010, 2 ss.

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*, n. 63, 2009, 5 ss.

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.