IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

Monográfico «Internet y redes sociales: un nuevo contexto para el delito»

ARTÍCULO

La regulación de los daños informáticos en el código penal italiano

Ivan Salvadori
Profesor de Derecho penal (Universidad de Barcelona)

Fecha de presentación: abril de 2013
Fecha de aceptación: junio de 2013
Fecha de publicación: junio de 2013

Resumen
En el presente trabajo se analiza la regulación de los delitos de daños informáticos introducidos en el Código penal italiano por la Ley número 48, de 18 de marzo de 2008, que ratifica y da ejecución al Convenio sobre Cibercrimen del Consejo de Europa. El objetivo es averiguar si la legislación penal italiana en materia de daños informáticos cumple con las recomendaciones internacionales y, en particular, si se adecua a las técnicas de protección adoptadas por otros legisladores europeos. En primer lugar se analizarán los tipos delictivos de daños a datos y a sistemas informáticos «privados» (artículos 635-*bis* y 635-*quater* del Código penal) y de daños a datos y a sistemas informáticos de carácter «publico» (artículos 635-*ter* y 635-*quinquies* del Código penal). Se pasará luego a estudiar su peculiar estructura típica y se determinarán los bienes jurídicos protegidos por los mencionados delitos. Por último, se formularán algunas consideraciones críticas en perspectiva de *lege ferenda*.

Palabras clave
Derecho penal informático, cibercrimen, daños informáticos, sabotaje informático, delitos de «atentado», delitos cualificados por el resultado, Ley número 48/2008, Código penal italiano

Tema
Derecho penal informático

Regulation of computer damage in Italian criminal law

Abstract

The article analyses the regulation of computer damage crimes as introduced into the Italian Criminal Code by Law 48, of 18 March 2008, which ratifies and brings into force the Convention on Cybercrime of the Council of Europe. The aim is to find out whether Italian criminal law on computer damage meets international guidelines and, in particular, whether it adapts to the protection techniques adopted by other European legislators. Firstly, the article analyses the crimes of criminal damage affecting "private" computer systems and data (articles 635-bis and 635-quater of the Criminal Code) and "public" computer systems and data (articles 635-ter and 635-quinquies). The article then goes on to study its peculiar structure and to determine the property legally protected against the aforementioned crimes. Finally, it provides some critical considerations with regard to lex ferenda.

Keywords

computer crime law, cybercrime, computer damage, computer sabotage, "attempted" crime, crime defined by the result, Law 48/2008, Italian criminal law

Subject

computer crime law

Introducción

Con la Ley número 48, de 18 de marzo de 2008, que ratifica y da ejecución al Convenio sobre Cibercrimen del Consejo de Europa (en adelante, CoC), el legislador italiano ha reformado algunos de los delitos informáticos (por ejemplo en materia de difusión de programas malware del artículo 615-*quinquies* del Código penal y de falsedades informáticas del artículo 491-*bis* del Código penal) que había introducido en el Código penal italiano (en adelante, c.p.) con la Ley número 547, de 23 de diciembre de 1993. Además de ello, también ha creado nuevos tipos delictivos para castigar las falsedades cometidas por el emisor de certificados de firma electrónica (artículo 495-*bis* del c.p.) y las estafas cometidas por este mismo (artículo 640-*quinquies* del c.p.).[1] Sin embargo, las principales novedades introducidas por la Ley número 48/2008 son las relativas a la normativa en materia de daños informáticos.

Para dar actuación a las disposiciones del Convenio sobre Cibercrimen en lo relativo a la interferencia en los datos (*data interference*) y en los sistemas informáticos (*system interference*), el legislador italiano ha distinguido, siguiendo las recomendaciones internacionales, entre daños a datos y daños a sistemas informáticos, y ha tipificado ambas conductas como delitos distintos. Sin embargo, en contra de lo que ha ocurrido en muchos países europeos (como, por ejemplo, en Alemania, Austria, España y Rumanía),[2] nuestro legislador no se ha limitado a introducir en el Código penal dos tipos delictivos autónomos en *subjecta materia*, sino que ha creado un complejo sistema normativo formado por cuatro normas distintas.

En los próximos párrafos se intentará averiguar si la legislación penal italiana en materia de daños informáticos cumple con las recomendaciones internacionales y, en particular, si se adecua a las técnicas de protección adoptadas en los últimos años por otros legisladores europeos (como, por ejemplo, el español y el alemán).

En primer lugar se analizarán los tipos delictivos de daños a datos y a sistemas informáticos «privados» (apartado 2),

1. Para un comentario sistemático de las principales novedades introducidas por la Ley 48/2008, véanse Sarzana (2008, pág. 1562 y sig.) y Picotti (2008b, pág. 437 y sig.). Respecto a los nuevos delitos de daños informáticos véase Salvadori (2012, pág 204 y sig.).
2. La bipartición entre daños a datos y a sistemas informáticos está prevista, por ejemplo, en la legislación penal alemana (§§ 303a y 303b del StGB), austriaca (§§ 126a y 126b del StGB), rumana (arts. 44 y 45 de la Ley de 21 de abril de 2003, núm. 161), portuguesa (arts. 3 y 4 de la Ley de 15 de septiembre de 2009, núm. 109) y española (arts. 264.1 y 2 del Código penal).

con particular atención al delito de daños a datos y programas del artículo 635-*bis* del c.p. (apartado 2.1), al delito de «sabotaje informático» del artículo 635-*quater* del c.p. (apartado 2.2) y al controvertido concepto de «ajenidad» de los datos y programas informáticos (apartado 2.3). En la segunda parte del trabajo se analizarán los delitos de daños a datos y a sistemas informáticos de carácter «publico» (apartado 3). En primer lugar se estudiará la estructura del artículo 635-*ter*, párrafo 1, del c.p. y del artículo 635-*quinquies*, párrafo 1, del c.p. (apartado 3.2), que se caracterizan por ser delitos de «atentado o emprendimiento» (*delitti di attentato* o *Unternehmensdelikte*).[3] Se pasará luego a analizar la problemática estructura de «delitos cualificados por el resultado» (*reati aggravati dall'evento*) utilizada en la tipificación de los artículos 635-*ter,* párrafo 2, del c.p. y 635-*quinquies,* párrafo 2, del c.p. (apartado 3.3). Para finalizar se formularán algunas consideraciones sobre el tratamiento sancionador, las circunstancias agravantes previstas en estos delitos (apartado 4) y los bienes jurídicos protegidos por estos delitos (apartado 5), y por último, como conclusión, se formularán algunas valoraciones criticas en perspectiva de *lege ferenda* (apartado 6).

2. Los daños a datos y a sistemas informáticos «privados»

2.1. Los daños a informaciones, datos y programas informáticos (artículo 635-bis del c.p.)

El delito de «daños a informaciones, datos y programas informáticos» del artículo 635-*bis* del c.p. castiga, con la pena de prisión de seis meses a tres años, a quien «destruyere, deteriorase, borrase, alterase o suprimiese informaciones, datos o programas informáticos ajenos».[4]

El objeto material del delito lo constituyen los datos, informaciones y programas informáticos ajenos. Respecto a la anterior formulación del artículo 635-*bis* del c.p., que había sido introducida en el Código penal mediante la Ley número 547/1993, el legislador italiano de 2008 ha suprimido la referencia a los sistemas informáticos o telemáticos, que, de acuerdo con la bipartición realizada tanto por el Convenio sobre Cibercrimen del Consejo de Europa como por la Decisión marco 2005/222/JAI, del Consejo de la Unión Europea, relativa a los ataques contra los sistemas de información, se protegen ahora mediante normas *ad hoc* (arts. 635-*quater* y 635-*quinquies* del c.p.).

No parece adecuada, sin embargo, la referencia que, junto con los datos y los programas informáticos, se hace a las *informaciones*, ya que su mención amplía de manera excesiva el ámbito de aplicación del delito y posibilita la subsunción en el artículo 635-*bis* del c.p. de los meros daños a informaciones contenidas en un documento de papel o que de todos modos no se puedan tratar mediante un programa informático.[5]

La formulación del tipo resulta adecuarse bastante a la del artículo 4 del Convenio sobre Cibercrimen. Respecto al anterior artículo 635-*bis* del c.p., que castigaba también la destrucción, el deterioro y la inutilización total o parcial de los datos, informaciones y programas informáticos ajenos, la nueva norma, que menciona expresamente los resultados ilícitos de cancelación, alteración y supresión de datos, resulta ser más correcta. Estos resultados típicos, que pueden ocasionarse también de manera omisiva, representan las distintas «modalidades» con las que puede manifestarse la agresión a la integridad y a la disponibilidad de los datos y de los programas informáticos.

La *alteración* consiste en una modificación del contenido de los datos informáticos.[6] De esta manera pueden ser subsumi-

3. Se trata de delitos que castigan la mera comisión de «actos dirigidos» a causar un resultado generador de lesión de un bien jurídico y cuya estructura objetiva coincide con la de la tentativa. Para un análisis de los problemas dogmáticos y político-criminales que plantea esta categoría de delitos, véanse en la doctrina italiana Gallo (1966 y 1987 [pág. 340 y sig.]), Zuccalá (1977, pág. 1225 y sig.), Grasso (1986, pág. 689 y sig.) y Padovani (1984, pág. 169 y sig.).
4. Artículo 635-*bis* del c.p.: «salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni e si procede d'ufficio».
5. En este sentido, véase Pecorella (2011, pág. 148 y sig.).
6. Respecto al análogo delito de alteración de datos (*Datenveränderung*), previsto en el párrafo 303a del Código penal alemán, véanse Wolff (2010, pág. 403) y Stree y Hecker (2010, pág. 2664).

dos en el nuevo artículo 635-*bis* del c.p. los daños causados mediante el empleo de programas malware que transformen o modifiquen el contenido de los datos informáticos.[7] Del mismo modo, podrán ser castigadas las alteraciones (o *defacement*) de páginas web que se sustancien en la modificación no autorizada de los datos informáticos que forman dichas páginas, o en la transformación de códigos fuente o del lenguaje de programación de un *software*. Por el contrario, no se podrá decir que existe alteración en los casos de instalación ilícita de programas espía (como, por ejemplo, *Spyware*, *Trojan Horse* y *Keylogger*), cuya función principal es la de memorizar los datos que se tratan y envían desde el ordenador «espiado» y transmitirlos al delincuente informático sin que haya ninguna modificación de su contenido.[8]

A diferencia del artículo 5 del CoC, el artículo 635-*bis* del c.p. no menciona los supuestos que consistan en la producción de daños, y tampoco, como requiere el artículo 4 de la Decisión marco 2005/222/JAI, aquellos que consistan en hacer inaccesibles los datos informáticos.

La decisión del legislador italiano de no castigar de manera expresa los hechos que consistan en «dañar» (*damaging*) datos informáticos ajenos no parece del todo correcta. El hecho de dañar datos o programas informáticos abarca casos que pueden ser subsumidos solo en parte en la conducta típica del *deterioro* de datos,[9] que consiste en disminuir o menoscabar el valor o la posibilidad de utilización de datos, informaciones o programas informáticos.

Críticas similares surgen con respecto a la decisión de no castigar los hechos que consistan en *hacer inaccesibles* datos informáticos, resultado expresamente mencionado en el artículo 4 de la Decisión marco 2005/222/JAI, que permitiría abarcar todas aquellas conductas (como, por ejemplo, el empleo no autorizado de programas de criptografía, la ilícita aposición de una contraseña a un archivo) cuyo efecto consiste en impedir, de manera permanente o temporal, el legitimo acceso a los datos a su titular. Sin embargo estos últimos casos podrían ser subsumidos en el resultado típico de *supresión* de datos informáticos.[10]

La *supresión* (*suppression*) de datos abarca no únicamente los hechos que consistan en una eliminación definitiva de los datos y que impidan cualquier posibilidad de recuperación de estos en el ordenador o soporte en los que estaban almacenados, sino también aquellos casos en que se impida el normal acceso a los datos a su legítimo titular. Piénsese, por ejemplo, en la sustitución de una contraseña o del nombre de un fichero, en el desplazamiento de un archivo a una carpeta o un directorio distinto o en la ocultación de los datos.[11]

La *cancelación* (*deletion*) consiste en hacer total y definitivamente irreconocible el contenido de los datos o de los programas informáticos.[12] Los datos se pueden cancelar tanto destruyendo o dañando los soportes en los que están almacenados como mediante su formateo. Del todo irrelevante será, a efectos penales, que los datos o los programas informáticos borrados puedan ser recuperados por su titular en otro soporte (por ejemplo, en un CD-ROM, en una copia de seguridad, etc.).[13]

El legislador italiano, a diferencia, por ejemplo, del español,[14] no ha considerado oportuno limitar la aplicación del tipo únicamente a los casos *graves* de daños a datos y programas informáticos. La *ratio* de esta cláusula «indefinida» es la de restringir el tipo delictivo para evitar que abarque también la simple alteración de datos cuando estos no tengan ningún valor o utilidad.

Sin embargo, a falta de una definición legal del concepto de «gravedad» de los daños producidos a datos y programas

7. *Cfr*. *Convention on Cybercrime. Explanatory Report*, 61. *(ETS n. 185)*.
8. En sentido similar, Hilgendorf, Frank y Valerius (2005, pág. 56).
9. *Op. cit.* Council of Europe (2001). Respecto a la interpretación de la conducta de deterioro de datos y de sistemas informáticos, véase en doctrina Pecorella (2006b, pág. 216 y sig.).
10. *Op.cit.* Council of Europe (2001).
11. Con respecto a la interpretación del tipo penal análogo de *Unterdrückung* prevista en el párrafo 303a del StGB, *cfr.* Hilgendorf, Frank y Valerius (2005, pág. 55), Wollf (2010, pág. 401-402) y Fischer (2010, pág. 2122).
12. Sobre el sentido de la cancelación (*Löschung*) de datos informáticos prevista por el párrafo 303a del StGB, véanse Hilgendorf, Frank y Valerius (2005, pág. 55) y Hoyer (2009, pág. 27, 3).
13. En sentido similar, véase en la doctrina alemana Zaczyk (2010, pág. 2481, marg. 7).
14. Sobre el nuevo delito de daños de datos informáticos del artículo 264.1 del Código penal español, véase I. Salvadori (2011, vol. LXIV, pág. 221-252).

informáticos, será competencia de los jueces la compleja tarea de determinar el criterio de selección de aquellos casos de daños que por su gravedad habría que considerar penalmente relevantes. Por lo tanto, la previsión de esta cláusula podría resultar contraria al principio fundamental de taxatividad, si bien *in bonam partem*.

2.2. Los daños a sistemas informáticos o telemáticos (artículo 635-*quater* del c.p.)

El delito de «daños a sistemas informáticos y telemáticos» del artículo 635-*quater* del c.p. castiga, con la pena de prisión de uno a cinco años, a quien «mediante las conductas mencionadas en el articulo 635-*bis* c.p. o a través de la introducción o la transmisión de datos, informaciones o programas informáticos destruya, dañe o inutilice en todo o en parte sistemas informáticos o telemáticos ajenos, u obstaculice de manera grave su funcionamiento».[15]

Se trata de un delito de resultado de medios determinados, puesto que el resultado tiene que producirse «mediante las conductas descritas en el art. 635-*bis* del c.p.» o «a través de la introducción o la transmisión de datos, informaciones o programas».

El primer supuesto típico, que se estructura como un tipo cualificado (*Qualifikationstatbestand*) respecto del tipo básico contenido en el artículo 635-*bis* del c.p., castiga los daños a sistemas informáticos o telemáticos ocasionados «mediante las conductas previstas en el art. 635-*bis* del c.p.», es decir, mediante «la destrucción, deterioro, cancelación, alteración o supresión de datos, informaciones y programas».[16] La formulación del delito es distinta a la del artículo 3 de la Decisión marco 2005/222/JAI y del artículo 5 del CoC, y no parece correcta en la parte en que califica como *conducta*, junto a las de *introducción* y de *transferencia* de datos mencionadas en la segunda parte del tipo, a los «hechos» típicos del artículo 635-*bis* del c.p., como si se tratase de un delito de acción.[17] Como se ha subrayado anteriormente, el artículo 635-*bis* del c.p. se caracteriza por ser un delito de resultado que castiga cualquier conducta (activa u omisiva) cuyo efecto causal consista en ocasionar un «daño» a través de una de las modalidades típicas de destrucción, cancelación, alteración o supresión de datos, informaciones o programas informáticos ajenos.

La segunda conducta tipificada en el delito del artículo 635-*quater* del c.p. castiga los sabotajes informáticos realizados «a través de la introducción o la transmisión de datos, informaciones o programas». La previsión de este subtipo, que se adecua al artículo 5 del CoC y al artículo 3 de la Decisión marco 2005/222/JAI, se justifica por la necesidad de castigar también los casos, cada día más frecuentes, de daños «lógicos» –es decir, que afectan a la parte del *software* de un sistema informático– llevados a cabo mediante las conductas neutras de introducción de datos en un sistema informático o de transmisión a través de la web o de un *hardware* (por ejemplo, USB, CD-ROM, etc.) de programas malware (como gusanos, virus, etc.).

El artículo 635-*quater* del c.p. describe el resultado típico del delito como «destruir, dañar, inutilizar total o parcialmente» u «obstaculizar gravemente el funcionamiento» de un sistema informático o telemático.

La formulación del primer resultado previsto por el tipo delictivo reproduce la conducta típica prevista en el artículo 635-*bis* del c.p.

El segundo resultado típico previsto en el artículo 635-*quater* del c.p. consiste, de acuerdo con la previsión del artículo 5 del CoC, en obstaculizar gravemente el funcionamiento de un sistema informático o telemático. Esta previsión, que parece incluir también la de interrupción (prevista en el artículo 3 de la Decisión marco 2005/222/JAI), se puede estimar correcta, puesto que permite superar aquellas lagunas normativas que impedían castigar, durante la vigencia del anterior artículo 635-*bis* del c.p., los daños «funcionales»

15. Artículo 635-*quater* del c.p.: «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».
16. Respecto al tipo análogo previsto en el § 303b, Abs. 1, n.1, del Código penal alemán, que castiga el *Computersabotage* cometido mediante daños a datos informáticos (§ 303a StGB), véanse Wolff (2010, pág. 418, marg. 2) y Stree y Hecker (2010, «303b StGB», pág. 2666). Considera que el § 303b n.1 del StGB constituye un delito agravado por el resultado (*erfolgsqualifiziertes Delikt*) Zaczyk (2010, pág. 2484). Una estructura similar tiene el nuevo delito de *sabotaje informático*, previsto en el artículo 264.2 del Código penal español.
17. Crítico también Picotti (2008a, pág. 713).

a un sistema informático o telemático.[18] Paradigmáticos en este sentido son los mencionados ataques de denegación de servicio (*denial of service* o *distributed denial of service attacks*), que impiden el correcto funcionamiento de un sistema informático si bien no causan en sentido estricto ningún daño a los datos y a los programas informáticos.

Los resultados funcionales, si bien coinciden muy a menudo con conductas dañosas «violentas», pueden producirse también en una fase posterior y autónoma respecto a estos.[19] Piénsese, por ejemplo, en la transmisión o en la introducción ilícita de un programa malware de tipo *worm* en un ordenador ajeno. En este caso la inutilización total o parcial del sistema informático puede verificarse *a posteriori* con el progresivo agotamiento de los recursos de la memoria ocupada por el «gusano».

Correcta y acorde con las recomendaciones del Consejo de Europa aparece la decisión político-criminal de limitar el ámbito penal del tipo a aquellos hechos que obstaculicen gravemente el funcionamiento de un sistema informático o telemático. La previsión de esta cláusula indeterminada permite excluir la relevancia penal de aquellos hechos que produzcan una interrupción de entidad muy leve a un sistema de información. Piénsese, por ejemplo, en el envío de un número limitado de mensajes de correo electrónico no deseados (*spam*), o en las protestas virtuales (*net-strike*) organizadas por grupos pequeños de usuarios, que no interfieren de manera relevante en el correcto funcionamiento de un servidor. En estos casos parece más correcto el recurso a los instrumentos penales y administrativos previstos por el código de la *privacy* (Decreto legislativo 196/2003) para el caso de que el *spammer* haya obtenido en internet direcciones de correo electrónico sin el consentimiento de sus titulares para enviar correos publicitarios no deseados. Esta conducta, en caso de que se cumplan todos los elementos típicos del delito de «tratamiento ilícito de datos» del artículo 167 del Decreto legislativo 196/2003, tendría que ser castigada de manera menos severa (prisión de seis a dieciocho meses) respecto a la pena prevista por el delito del artículo 635-*quater* del c.p.[20]

Resulta sorprendente, sin embargo, que queden excluidos del ámbito de aplicación del artículo 635-*quater* del c.p. los daños físicos, esto es, aquellos que se cometan contra la parte del soporte físico de un sistema informático.[21]

Efectivamente, la norma se refiere solamente a aquellos daños lógicos cometidos mediante las «conductas» de destrucción, deterioro, cancelación o a las conductas de introducción o transmisión de datos, informaciones o programas informáticos. Por lo tanto, solo se podrá reconducir a este delito aquellos casos de daños físicos que se verifiquen (de manera indirecta) a través de modalidades lesivas de tipo «lógico», es decir, mediante datos o contra datos o programas informáticos. Piénsese, por ejemplo, en la introducción o en la transmisión de un virus que obstaculice indirectamente el correcto funcionamiento del ventilador de enfriamiento de un sistema informático infectado, inutilizando en parte, u obstaculizando, el correcto funcionamiento del sistema. En este caso nos encontraríamos frente a una evidente disparidad de tratamiento, puesto que los casos de daños «físicos» causados a sistemas informáticos se castigarían con la pena (mucho más leve) prevista por el artículo 635 del c.p. (de reclusión de hasta un año o multa de hasta 309 euros) en lugar de la pena más grave establecida por los daños «lógicos» del artículo 635-*quater* del c.p. (prisión de uno a cuatro años), a pesar de que los efectos sobre el funcionamiento del sistema informático afectado podrían ser idénticos.

2.3. El concepto de «ajenidad» de los datos, informaciones y programas informáticos

Los «hechos» típicos de destrucción, deterioro, cancelación, alteración o supresión de informaciones, datos y programas informáticos previstos en el delito del artículo 635-*bis* del c.p. constituyen eventos técnicamente neutros, que

18. Esta laguna había sido subrayada ya en doctrina por Picotti (2000, pág. 8 y sig.). En contra Pecorella (2006b, pág. 219 y sig.), según la cual las alteraciones de tipo funcional podían ser abarcadas mediante la conducta tipificada de «inutilización total o parcial» de un sistema informático o telemático.
19. En este sentido, Picotti (2008a, pág. 445). De manera más general, con respecto al delito de daños a cosas del artículo 635 del c.p., véase Bricola (1962, pág. 606), según el cual el resultado dañoso tiene que considerarse *in re ipsa* respecto a la conducta violenta.
20. Sobre la aplicación del tratamiento ilícito de datos personales del artículo 167 del Decreto legislativo 196/2003 por el envío de correos electrónicos no deseados, véase Salvadori (2008, pág. 354 y sig.).
21. *Cfr.* Pecorella (2011, pág. 150).

no presentan en sí mismos connotación ilícita alguna. En este sentido resulta paradigmática la amplia definición de «tratamiento de datos» que proporciona el artículo 4, párrafo 1, letra a) del llamado *código de la privacy* italiano (Decreto legislativo 196/2003) que incluye, entre las conductas lesivas que pueden tener como objeto los datos (personales), también su modificación, bloqueo, *cancelación* y *destrucción*.

Por lo tanto, resulta difícil delimitar, sin otros elementos típicos, la esfera de las conductas lícitas que recaen sobre los datos informáticos respecto a los comportamientos ilícitos merecedores de sanción penal, ya que falta un requisito intrínseco de ilicitud en los resultados de daños tipificados en el artículo 635-*bis* del c.p.

No parece posible determinar el carácter ilícito de los daños sobre la base de la ausencia de consentimiento por parte del titular de los datos o de los programas informáticos dañados.[22] Si lo hiciéramos, nos encontraríamos ante una ilógica presunción de tipicidad de todas las operaciones que causen un efecto similar a las conductas previstas en el delito de daños causados a informaciones, datos y programas, cuyo carácter antijurídico habría que excluir en cuanto se constate la presencia de la causa de justificación del consentimiento de la víctima. Esto produciría una parálisis de las operaciones cotidianas de tratamiento de datos y programas realizadas por parte de sujetos públicos o privados en el ámbito laboral, jurídico, económico o social, que en abstracto tendrían que ser subsumidas en el artículo 635-*bis* del c.p.

Con el objetivo de superar las dificultades a la hora de distinguir entre los casos de daños a datos penalmente relevantes de los que no lo son, el legislador italiano, pese a las fuertes críticas de la doctrina, ha considerado oportuno recurrir al dudoso requisito de la *ajenidad* de los datos, informaciones y programas informáticos.[23] Esta previsión representa una anomalía, no solo respecto a las fuentes internacionales, sino también en referencia al panorama jurídico europeo donde, a excepción de España, la referencia al carácter ajeno de los datos o programas se ha omitido, requiriendo de manera más correcta que los daños a los datos se lleven a cabo «sin derecho» o «sin autorización». Estas cláusulas de ilicitud expresa, que no requieren necesariamente la existencia de un derecho de propiedad o de posesión del sujeto pasivo sobre los datos informáticos dañados, permiten recurrir, a la hora de delimitar el hecho típico, a todas las normas extrapenales que regulan las actividades legítimas sobre los datos.[24]

Sin duda, por lo tanto, habría sido más correcta la previsión por parte del legislador italiano de una cláusula de ilicitud expresa, para delimitar así el ámbito de aplicación del delito de daños a datos informáticos llevados a cabo mediante conductas «no autorizadas».[25]

Esta ha sido, por ejemplo, la técnica de formulación adoptada por los legisladores rumano (arts. 44 y 45 de la Ley 196/2003) y belga (art. 550-*ter* del Código penal), que castiga los daños cometidos sin autorización («sachant qu'il n'y est pas autorisé»)[26] y por el legislador español, que en el artículo 264, párrafos 1 y 2, del Código penal castiga los daños a datos y a sistemas informáticos cometidos «sin autorización».[27] Muy similar es la técnica adoptada por el legislador alemán (§§ 303a, 303b StGB), si bien este ha preferido emplear el adverbio «rechtswidrig» (de manera antijurídica).[28] Según destacada doctrina, esta cláusula de ilicitud no constitui-

22. En este sentido véase, anteriormente, Picotti (2000, pág. 19) y, más recientemente, Picotti (2008a, pág. 444).
23. Véanse, bajo la vigencia del anterior artículo 635-*bis* del c.p., introducido en el Código penal italiano mediante la Ley 547/1993, las observaciones críticas de Picotti (2000, pág. 19); en sentido similar, Pecorella (2006b, pág. 204-211).
24. Sobre la distinción entre cláusulas de ilicitud expresa y especial, véase Pulitanò (1967, pág. 65 y sig.).
25. En este sentido, véase también la disposición en materia de daños ocasionados a datos y programas informáticos prevista por la Recomendación R (89) 9 del Consejo de Europa, que requiere a los estados miembros que castiguen «the erasure, damaging, deterioration or suppression of computer data or computer programs without right».
26. Para un análisis del artículo 550-*ter* del Código penal belga, véase Meunier (2001, pág. 630 y sig.).
27. Es similar la técnica adoptada por el legislador portugués, que en la transposición del Convenio sobre Cibercrimen del Consejo de Europa mediante la Ley número 109, de 15 de septiembre de 2009, ha castigado los daños informáticos (arts. 4 y 5 de dicha ley) cometidos «sem permissão legal ou sem para tanto estar autorizado pelo proprietário».
28. Respecto a la interpretación del adverbio «rechtswidrig» y sobre su controvertida colocación en el ámbito de la categoría de la tipicidad o de la antijuridicidad, véanse, en el debate doctrinal alemán, las consideraciones de Hilgendorf (1994), «Tatbestandsprobleme bei der Datenveränderung nach § 303a StGB», *Juristische Rundschau*, pág. 478; y de Dreher, Lackner y Kühl (2011, «303a StGB», pág. 1412).

ría un elemento de la antijuridicidad (*Rechtswidrigkeit*), sino de la tipicidad (*Tatbestandsmerkmal*) del delito.[29]

3. Los daños a datos y a sistemas informáticos «de utilidad pública»

3.1. Sobre la peculiar técnica de formulación de los delitos

Al dar actuación al Convenio sobre Cibercrimen del Consejo de Europa, el legislador italiano no se ha limitado –como han previsto muchos legisladores europeos (como, por ejemplo, el alemán, el español y el austriaco)– a distinguir entre los daños ocasionados a datos y aquellos otros ocasionados a sistemas informáticos, sino que ha ido más allá castigando de manera autónoma los «daños ocasionados a informaciones, datos y programas informáticos utilizados por el Estado o por otra entidad pública o que de todos modos resulten ser de utilidad pública» (art. 635-*ter* del c.p.) y los «daños ocasionados a sistemas informáticos o telemáticos de utilidad pública» (art. 635-*quinquies* del c.p.).

La primera crítica que hay que formular a la decisión del legislador italiano es la de utilizar expresiones distintas para definir «objetos» que revisten la misma relevancia pública, puesto que ello no queda justificado desde un punto de vista político-criminal. En lugar de la compleja y controvertida expresión «utilizados por el Estado o por otra entidad pública, o a ellos pertenecientes, o de todos modos de utilidad pública» para calificar los «objetos» sobre los que recaen los efectos lesivos tipificados en el artículo 635-*ter* del c.p., habría sido mejor que el legislador hubiera empleado la expresión, mas sintética, de «utilidad pública», que ha empleado en el artículo 635-*quater* del c.p.[30]

Más criticable aún es la decisión de tomar como modelo –para tipificar los delitos de daños ocasionados a datos y a sistemas informáticos «públicos»– el delito de «atentado contra instalaciones de utilidad pública» del artículo 420 del c.p. (parcialmente derogado por el artículo 6 de la Ley 48/2008) y no, como habría sido más correcto, el delito de daños causados a datos informáticos del artículo 635-*bis* del c.p. y de sabotaje informático del artículo 635-*quater* del c.p.

De la misma manera que el mencionado artículo 420, párrafo 2, del c.p., tanto el artículo 635-*ter*, párrafo 1, del c.p. como el 635-*quinquies*, párrafo 1, del c.p. se caracterizan por su peculiar estructura de los llamados delitos «de atentado», «de emprendimiento» o «de preparación» («actos dirigidos a...») y, por consiguiente, por la anticipación de la tutela penal.

La estructura de los artículos 635-*ter*, párrafo 2, del c.p. y 635-*quinquies*, párrafo 2, del c.p. es igual a la del derogado párrafo tercero del artículo 420 del c.p. De esta manera, el legislador ha introducido en este complejo sistema normativo que regula la materia de los daños informáticos dos nuevos delitos que se caracterizan por presentar una peculiar estructura de «delitos cualificados por el resultado» (*reati aggravati dall'evento*).

3.2. Los «delitos de atentado» contra datos y sistemas informáticos de utilidad pública (artículo 635-*ter*, párrafo 1, del c.p. y artículo 635-*quinquies*, párrafo 1, del c.p.)

El primer párrafo del artículo 635-*ter* del c.p. castiga, con la pena de prisión de uno a cuatro años, el hecho dirigido a «destruir, deteriorar, borrar, alterar o suprimir» informaciones, datos o programas informáticos de relevancia pública.

El artículo 635-*quinquies*, párrafo 1, del c.p. castiga, con la pena de prisión de uno a cuatro años, los actos dirigidos a destruir, dañar o inutilizar, en todo o en parte, sistemas informáticos o telemáticos «públicos» o a obstaculizar gravemente su funcionamiento, cuando estos se cometan mediante las modalidades típicas descritas en el artículo 635-*quater* del c.p. Ambos delitos se caracterizan por su estructura de «delitos de atentado».[31] Para no extender excesivamente el ámbito de aplicación de estos delitos parece más correcto entender que el umbral de la relevancia penal de los atentados contra datos y sistemas informáticos de «utilidad pública» coincide con el de la tentativa de los correspondientes delitos comunes de «daños a informacio-

29. En doctrina, véanse Dreher, Lackner y Kühl (2011, pág. 1412), Hilgendorf (1996, pág. 892), Hoyer (2009, pág. 12) y Hilgendorf, Frank y Valerius (2005, pág. 54).
30. *Cfr.* Picotti (2008a, pág. 715).
31. Sobre la estructura de los delitos de «consumación anticipada», véase Delitala (1930, pág. 178 y sig.); equiparan los delitos de atentado a los delitos de consumación anticipada también Nuvolone (1975, pág. 390 y sig.) y Mazzacuva (1983, pág. 181).

nes, datos y programas informáticos» del artículo 635-*bis*, párrafo 1, del c.p. y de «daños a sistemas informáticos o telemáticos» del artículo 635-*quater*, párrafo 1, del c.p. Por lo tanto serán penalmente relevantes únicamente aquellos actos que, sobre la base de un criterio de *prognosis póstuma* (*ex ante*), resulten ser objetivamente idóneos y dirigidos de manera inequívoca a crear un peligro concreto para el bien jurídico protegido (véase *infra* apartado 5).[32] Por el contrario, habrá que excluir la punibilidad de estos delitos en fase de tentativa, al no ser compatible con su naturaleza de delitos de «atentado» o de «*emprendimiento*» (*delitti di attentato*).[33]

3.3. La estructura de los artículos 635-*ter*, párrafo 2, y 635-*quinquies*, párrafo 2, del c.p.

Sobre la base del artículo 635-*ter,* párrafo 2, del c.p., el delito de atentado contra informaciones, datos y programas informáticos de «utilidad pública» (art. 635-*ter,* párrafo 1, del c.p.) se castigará con la pena de prisión de tres a ocho años si de su comisión se deriva la destrucción, deterioro, cancelación, alteración o supresión de informaciones, datos o programas informáticos.[34]

El artículo 635-*quinquies*, párrafo 2, del c.p. establece que el delito de «atentado» contra sistemas informáticos o telemáticos «públicos» (art. 635-*quinquies*, párrafo 1, del c.p.) se castigue con la pena de prisión de tres a ocho años, si de su comisión se deriva la destrucción de, o el daño a un sistema informático o telemático, o este resulte en todo o en parte inutilizado.[35]

En ambos artículos el legislador italiano ha empleado una expresión («si del hecho se derivase») propia de los «delitos agravados por el resultado» (*reati aggravati dall'evento*).[36] Sin embargo, para poder incluir estas normas en la categoría de los «delitos agravados por el resultado» hay que analizar también su estructura típica.

Los artículos 635-*ter*, párrafo 2, del c.p. y 635-*quinquies*, párrafo 2, del c.p. configuran respectivamente como agravante el resultado de daños ocasionados a datos, informaciones y programas informáticos y el de daños ocasionados a sistemas informáticos o telemáticos de utilidad pública. El resultado típico que tiene que producirse para que se consideren cometidos los delitos de los artículos 635-*ter,* párrafo 2, del c.p. y 635-*quinquies,* párrafo 2, del c.p. ha de ser abarcado por el dolo del hecho típico previsto en el primer párrafo de cada delito. Por ello, no nos hallamos ante auténticos «delitos cualificados por el resultado», sino ante tipos delictivos autónomos. Por lo tanto, desde un punto de vista práctico, el resultado de «destrucción, deterioro, cancelación, alteración o supresión» en un caso, y de «destrucción y daño» de datos y de sistemas de utilidad pública en el otro, tiene que considerarse como un elemento constitutivo de un delito consumado autónomo, y no como un elemento circunstancial de las conductas de atentado. El resultado producido no podrá ser objeto de una ponderación de las circunstancias, tal como establece el artículo 59 del c.p.[37]

32. Sobre la necesidad de que los actos que constituyen un «delito de atentado» o «de emprendimiento» (*delitti di attentato*) causen un concreto peligro al bien jurídico protegido, véase Gallo (1987, pág. 340 y sig.). Sobre la estructura de los delitos de peligro concreto, véanse, más en general, Angioni (1994, pág. 206 y sig., y 1983, pág. 177) y Parodi Giusino (1990, pág. 318 y sig.). En la doctrina alemana, véanse, *ex pluribus*, Zieschang (1998, pág. 384-389); Wohlers (2000, pág. 311-318) y Roxin (2006 pág. 423-426, marg. 147-152).
33. En doctrina, véanse Petrocelli (1955, pág. 52); M. Gallo (2003), *Appunti di diritto penale. Le forme di manifestazione del reato*, Turín, pág. 64 y sig.; Romano (2004, pág. 602); Marinucci y Dolcini (2001, pág. 591); Padovani (2008, pág. 277) y Fiandaca y Musco (2012, pág. 470).
34. Artículo 635-*ter*, párrafo 2, del c.p.: «se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni».
35. Artículo 635-*quinquies*, párrafo 2, del c.p.: «se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni».
36. Sobre la controvertida naturaleza de los delitos agravados por el resultado, véanse, *ex pluribus*, Grosso (1963, pág. 442 y sig.); Concas (1967, pág. 809 y sig.); Vassalli (1975, pág. 3 y sig.); Dolcini (1979), «L'imputazione dell'evento aggravante. Un contributo di diritto comparato», *Rivista italiana di diritto e procedura penale*, pág. 755 y sig.; Tagliarini (1979); Ardizzone (1984); Gallo (1990, pág. 410 y sig.); Bondi (1994, pág. 1460 y sig., y 1999, pág. 49 y sig.) y Preziosi (2000).
37. En este sentido, negando que los «delitos de emprendimiento» (*delitti di attentato*) puedan considerarse delitos cualificados por el resultado y que, por lo tanto, el resultado típico producido tenga que considerarse como simple elemento circunstancial del delito, véase Gallo (1990, pág. 419-422). En contra, Vassalli (1975, pág. 41). Más en general, respecto a los criterios elaborados por la doctrina para establecer cuándo hay un delito autónomo o un delito circunstancial, véanse Gallo (1949, pág. 560 y sig.), Guerrini (1988) y Melchionda (2000, pág. 558 y sig., en especial pág. 565-576).

4. Tratamiento sancionador y circunstancias agravantes

El tipo básico del delito de daños ocasionados a informaciones, datos y programas informáticos del artículo 635-*bis*, párrafo 1, del c.p. se castiga con la pena de prisión de seis meses a tres años, mientras que los tipos agravados del segundo párrafo, introducidos ya mediante la anterior Ley número 547/1993, se castigan con la pena de prisión de uno a cuatro años.

Presenta escasa relevancia práctica la circunstancia agravante de haber cometido los daños a datos y a sistemas informáticos tanto públicos como privados «con violencia sobre las personas o con amenazas». El legislador parece no haber tenido en cuenta que hoy en día la mayoría de los ataques informáticos se realizan a través de las redes telemáticas y en especial de internet, sin la necesidad de un contacto físico con los sistemas informáticos y con las personas que en su caso velan por la seguridad de estos sistemas.

Con toda seguridad, presenta una mayor relevancia práctica la circunstancia agravante establecida para todos los tipos de daños ocasionados a datos y a sistemas informáticos cuando estos se cometan «con abuso de la función de operador de sistema».[38] Sin embargo hay que subrayar que el concepto de «operador de sistema», que no se ajusta al lenguaje informático, podría abarcar a todos aquellos sujetos que, por distintas razones, «operan» sobre un sistema informático.[39] Hubiera sido mejor, por lo tanto, sustituir esta discutible expresión con la de «administrador de sistema» (*system administrator*), que con toda seguridad resulta ser más adecuada a la finalidad de abarcar a todos aquellos técnicos informáticos que, por el hecho de tener un control sobre las fases de un proceso de elaboración de datos informáticos, pueden acceder con mayor facilidad a los datos y a los programas contenidos en los sistemas informáticos en los que operan. Y precisamente de esta relación privilegiada con los sistemas informáticos –además de la naturaleza particularmente confidencial de sus tareas– deriva aquella especial peligrosidad de las conductas que justifica un tratamiento sancionador más grave en los casos de daños informáticos cometidos por los administradores de los sistemas.

La formulación de las circunstancias agravantes previstas por los delitos de «atentado» contra datos y sistemas informáticos de «utilidad pública» (arts. 635-*ter*, párrafo 3, y 635-*quinquies*, párrafo 3, del c.p.) y por los delitos de daños ocasionados a sistemas informáticos y telemáticos (art. 635-*quater*, párrafo 2, del c.p.) es idéntica a la del artículo 635-*bis*, párrafo 2, del c.p., excepto por la falta de determinación de la entidad del aumento de pena.[40] Para estos casos, sobre la base de la regla establecida por el artículo 64 del c.p., habrá que apreciar un aumento de pena en los subtipos agravados de hasta un tercio respecto a la pena prevista por el correspondiente tipo básico.

El tratamiento sancionador previsto para los delitos (consumados) de daños ocasionados a datos y a sistemas informáticos de «utilidad pública» previstos en los artículos 635-*ter*, párrafo 2, y 635-*quinquies*, párrafo 2, del c.p., que se caracterizan por su severidad (pena de reclusión de tres a ocho años), aparece del todo «autónomo» respecto al tratamiento más benévolo previsto para los casos de atentado contra datos y sistemas informáticos (reclusión de uno a cuatro años). Además de resultar desproporcionado y excesivamente severo, este tratamiento es contrario a las propias recomendaciones internacionales que, tipificando de manera autónoma los daños ocasionados a datos y a sistemas informáticos, requieren implícitamente que estos vengan castigados de manera distinta. Por el contrario, la pena prevista por el delito (consumado) de daños ocasionados a datos de utilidad pública del artículo 635-*ter*, párrafo 2, del c.p. resulta ser no solamente más grave que la del delito de daños ocasionados a sistemas informáticos y telemáticos «privados» del artículo 635-*quater* del c.p., sino además idéntica a la del tipo de daños a sistemas informáticos «públicos» (art. 635-*quinquies*, párrafo 2, del c.p.).

38. La circunstancia agravante del abuso de «actuar en calidad de operador de un sistema informático» se aplica también a los delitos de «acceso ilícito a un sistema informático o telemático» (art. 615-*ter* del c.p.), de «posesión y difusión ilícita de códigos de acceso a sistemas informáticos o telemáticos» (art. 615-*quater* del c.p.), de «interceptación o interrupción ilícita de comunicaciones informáticas o telemáticas» (art. 617-*quater* del c.p.), de «instalación de aparatos aptos para interceptar, impedir o interrumpir comunicaciones informáticas o telemáticas» (art. 617-*quinquies* del c.p.), de «falsificación, alteración o supresión del contenido de comunicaciones informáticas o telemáticas» (art. 617-*sexies* del c.p.) y de «estafa informática» (art. 640-*ter* del c.p.).
39. En este sentido, véanse Mucciarelli (1996, pág. 102) y Pecorella (2006a, pág. 4330, y 2006b, pág. 121 y sig.).
40. En sentido crítico, véase Picotti (2008a, pág. 713).

Por ello, es criticable la decisión político-criminal de equiparar desde un punto de vista sancionador los ilícitos contenidos en los artículos 635-*ter* y 635-*quinquies* del c.p., puesto que el desvalor de los ataques dirigidos contra sistemas informáticos de utilidad pública (art. 635-*quinquies* del c.p.) es muy superior a la de los daños ocasionados a datos, informaciones y programas informáticos «públicos» del artículo 635-*ter* del c.p. Es evidente, por lo tanto, la diferencia sancionadora respecto a los tipos básicos de daños ocasionados a datos «privados» (pena de reclusión de seis meses a tres años) y de los ocasionados a sistemas informáticos «privados» (pena de reclusión de uno a cinco años) de los artículos 635-*bis* y 635-*quater* del c.p.

En perspectiva de *lege ferenda*, sería oportuno que el legislador, de acuerdo con las recomendaciones internacionales, diferenciase el tratamiento sancionador –sobre la base de su distinto desvalor– de los ataques informáticos cometidos contra los datos y los sistemas informáticos de naturaleza «privada» y aquellos de naturaleza «pública».

5. Los bienes jurídicos protegidos

Parte de la doctrina, valorando sobre todo la colocación sistemática de los delitos de daños informáticos en el Código penal, ha afirmado que el bien jurídico protegido por estas normas es el valor patrimonial de los bienes informáticos (datos, informaciones, programas y sistemas informáticos).[41] Sin embargo, de esta manera se ha sobrestimado su colocación sistemática sin tener en cuenta que para determinar el interés jurídico protegido, en la relación entre el «título» («sección» o «capítulo») y el texto normativo, debe predominar siempre este último por ser más vinculante y de mayor riqueza descriptiva.[42] La colocación sistemática del delito es solamente uno de los criterios hermenéuticos a disposición del intérprete para confirmar lo que se ha obtenido desde la interpretación del texto normativo.[43] En la determinación del interés jurídico protegido por la norma el intérprete tiene que estar necesariamente vinculado al contenido del «hecho» típico.[44]

Sobre la base del análisis de los «hechos» tipificados por los delitos de daños informáticos emerge que el bien jurídico protegido no es el patrimonio del propietario de los datos o de los sistemas informáticos dañados (que queda como un bien jurídico secundario), sino la integridad y la disponibilidad de los datos y de los sistemas informáticos.[45]

6. Consideraciones críticas finales y perspectivas de *lege ferenda*

El loable objetivo del legislador italiano de dar actuación a las disposiciones del Convenio sobre Cibercrimen en lo relativo a los daños informáticos no se ha conseguido de manera satisfactoria.

En primer lugar el legislador no ha suprimido la referencia al controvertido concepto de «ajenidad» de los datos, informaciones y programas informáticos. La referencia a esta expresión, en el contexto de la informática, crea muchos problemas para determinar tanto quién es la persona ofendida como el interés protegido. Es muy complejo aplicar a «objetos» informáticos conceptos tradicionales propios del derecho civil, como los de propiedad y de posesión.

En perspectiva de *lege ferenda*, sería oportuno que el legislador sustituyese el controvertido requisito de la ajenidad de

41. En este sentido, bajo la vigencia del anterior artículo 635-*bis* del c.p., Rinaldi (1996, pág. 134, nota 2); Pica (1999, pág. 86-87), según el cual «l'inquadramento sistematico [dell'art. 635-*bis* c.p.] appare corretto, anche perché non vi è dubbio che la norma vuole offrire tutela al bene informatico sotto il profilo patrimoniale». En sentido similar, Manes (en VV. AA., 2006, pág. 567), Scopinaro (2007, pág. 206) y Fiandaca y Musco (2007, pág. 144). Determina en la propiedad y el goce de datos y sistemas informáticos el bien jurídico protegido por los delitos de daños informáticos Mantovani (2009, pág. 136).
42. Angioni (1983, pág. 12).
43. Angioni (1983, pág. 13). En sentido similar, Donini (1996, pág. 125).
44. Sobre la función del «hecho típico» en la teoría del delito, véanse Delitala (1930), Marinucci (1983, pág. 1237 y sig.), Pagliaro (1960) y Donini (1996, pág. 108 y sig.).
45. En este sentido, véanse ya Conseil de l'Europe, *Criminalité informatique*, pág. 44; Council of Europe, *Explanatory Report*, 60; también Commonwealth (2002), *Model Law on Computer and Computer related Crime*, en ‹http://www.thecommonwealth.org›. En la doctrina alemana véanse Sieber (1986); Hilgendorf, Frank y Valerius (2005, pág. 54 y 57) y Wolff (2010, pág. 390 y 418); en la doctrina italiana, Picotti (2004, pág. 73).

los datos, requiriendo, de acuerdo con la técnica adoptada por otros legisladores europeos, que las conductas dañosas se lleven a cabo «sin autorización».

Por otra parte, suscita mucha perplejidad, desde un punto de vista político-criminal, la decisión de formular los daños ocasionados a datos y a sistemas informáticos «públicos» como delitos de «atentado». El empleo de esta técnica de protección en el ámbito de la criminalidad informática es contrario al principio de proporcionalidad.[46] Este fundamental principio requiere que entre el grado de la anticipación de la protección penal y la importancia del bien jurídico protegido exista una cierta proporción.[47] Por lo tanto, la incriminación de hechos que se caractericen por una peligrosidad no suficientemente elevada es únicamente admisible en aras a la protección de un interés jurídico fundamental como, por ejemplo, el del sistema de derechos e instituciones primordiales del Estado, sin los cuales este perdería su identidad de Estado social de Derecho.[48]

El recurso a la técnica de los delitos de «atentado» para sancionar la puesta en peligro de los bienes jurídicos cuyo nivel de importancia no es suficientemente alto no resulta adecuado, ya que infringe el principio de proporcionalidad.[49] Los delitos de «atentado» (o «de emprendimiento») contra los datos y los sistemas informáticos «de utilidad pública» permiten la incriminación de conductas que en realidad son meramente preparatorias y que no representan, en la mayoría de los casos, una seria amenaza para un bien jurídico fundamental ni son indispensables para la sobrevivencia del sistema político-constitucional o de la propia sociedad. La decisión político-criminal de anticipar la protección penal a los actos de preparación resulta completamente desproporcionada.

En la sociedad de la información, los intereses jurídicos emergentes de *la integridad y la disponibilidad de los datos y de los sistemas informáticos* (así como el de la *intimidad informática*)[50] han adquirido una notable dimensión y relevancia social. Se trata de bienes jurídicos que merecen ser protegidos por el derecho penal y que necesitan de su protección debido a la ineficacia o la insuficiencia de los medios alternativos de protección, tanto técnicos (contraseña, cortafuegos, etc.) como organizativos (códigos deontológicos, reglamentos, *policy*, etc.). Una protección efectiva resulta indispensable para garantizar el interés colectivo de la *seguridad informática*,[51] además de la certeza, rapidez y normal desarrollo de las relaciones sociales, económicas y jurídicas que cada día con más frecuencia se llevan a cabo a través de medios informáticos. Pese a su gran importancia, estos intereses jurídicos no poseen, en la jerarquía de los valores propios de un ordenamiento democrático, una importancia tal que justifique una protección que recurra a la técnica de los delitos de consumación anticipada o de preparación (atentado).

Hay que criticar, por lo tanto, la decisión político-criminal del legislador italiano de proteger los datos, las informaciones, los programas y los sistemas informáticos «públicos» a través del recurso a la técnica de los delitos de «atentado». El mismo resultado se habría podido conseguir, sin incurrir en evidentes problemas hermenéuticos, previendo una circunstancia agravante especial autónoma para los delitos de daños ocasionados a datos y sistemas informáticos.[52]

En perspectiva de *lege ferenda*, es oportuno que el legislador, de acuerdo con las indicaciones internacionales y con las decisiones de muchos legisladores europeos (por ejemplo, los legisladores alemán, español, y austriaco) for-

46. Sobre el fundamento constitucional del principio de proporción, véanse Angioni (1983, pág. 176), Vassalli (1991, pág. 699 y sig.), Palazzo (1992, pág. 453 y sig.) y Marinucci y Dolcini (2001, pág. 519, en particular la nota 99); en la doctrina española, véase Mir Puig (2009, pág. 1357 y sig.).
47. Según Angioni (1983, pág. 176), «Tanto più importante [...] è il bene offendibile dal reato, tanto più è legittimamente anticipabile la sua tutela e viceversa».
48. Angioni (1983, pág. 12).
49. Véase Angioni (1983, pág. 180 y sig., pág. 203 y sig.).
50. Sobre este nuevo interés jurídico, véanse Picotti (2004, pág. 78) y Salvadori (2008), «L'esperienza giuridica degli Stati Uniti in materia di hacking e cracking», *Rivista italiana di diritto e procedura penale*, núm. 3, pág. 1279 y sig.
51. Sobre la seguridad informática, o interés merecedor de protección penal, véanse las consideraciones de Picotti (2004, pág. 70 y sig.).
52. En este sentido, véase, por ejemplo, el § 303b, párrafo 2, del Código penal alemán, que establece un aumento de pena en los casos de daños a un sistema informático de esencial importancia para la Administración pública. Es similar la formulación del artículo 264, párrafo 3.2, del Código penal español, que castiga, de acuerdo con el artículo 7, párrafo 2, de la Decisión marco 2005/222/JAI, los ataques a los datos y a los sistemas informáticos que afecten a intereses esenciales de la sociedad.

mule los delitos de daños ocasionados a datos y a sistemas informáticos como *delitos de resultado*. De esta manera se evitaría una excesiva anticipación del ámbito de aplicación y se garantizaría, al mismo tiempo, la punibilidad de la tentativa.

La hipertrofia normativa en materia de daños informáticos no parece el instrumento idóneo para abarcar todas las modalidades lesivas que inciden sobre la integridad y la disponibilidad de los datos y de los sistemas informáticos. En los tipos delictivos de daños a sistemas informáticos (arts. 635-*quater* y 635-*quinquies* del c.p.) solo se pueden subsumir aquellos hechos de agresión «lógica» a datos y programas que causen un daño funcional a sistemas de información. Por el contrario, quedan excluidos los daños físicos cometidos contra la parte del *hardware* de un sistema informático o telemático, que en consecuencia podrán ser subsumidos solamente en el delito menos grave de daños a las cosas del artículo 635 del c.p., a pesar de que puedan provocar los mismos efectos sobre la funcionalidad del sistema.

Tomando como modelo la legislación alemana, el legislador italiano podría incluir dentro del delito de daños ocasionados a sistemas informáticos y telemáticos un «subtipo» *ad hoc* para castigar también los daños de carácter «físico».[53]

Teniendo en cuenta los nuevos intereses jurídicos protegidos en la sociedad de la información, sería también recomendable que el legislador cambiase la colocación de los delitos de daños informáticos y los situase fuera de los delitos contra el patrimonio. En este sentido podría introducir en el Código penal un nuevo título dedicado al bien jurídico de la *seguridad informática*, en el que colocar todos los delitos que lesionen o pongan en peligro la intimidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, como, por ejemplo, el acceso ilícito a un sistema informático, la detención y la difusión de códigos de acceso, la interceptación de datos informáticos, los daños informáticos, etc.[54]

En conclusión, sería oportuna una reforma del sistema normativo italiano en materia de daños informáticos para adecuarlo, no solo desde un punto de vista formal, sino también sustancial, a las obligaciones internacionales, tal como requiere expresamente la Constitución italiana (arts. 10, 11 y 117). Para dar una correcta actuación a estas obligaciones será necesario que en el futuro el legislador italiano tome más en cuenta la importante contribución de la experiencia jurídica extranjera, que constituye un útil instrumento para verificar la corrección de las técnicas de protección que hay que adoptar. Al mismo tiempo tendrá que mantenerse en el camino trazado por los principios constitucionales fundamentales en materia penal (legalidad, ofensividad, proporcionalidad y subsidiariedad),[55] que no pueden ser sacrificados amparándose en que hay que cumplir, de manera formal, con las obligaciones internacionales en materia de lucha contra la criminalidad informática.

53. El § 303b, párrafo 1, núm. 3, del Código penal alemán (StGB) castiga con la pena de prisión de hasta tres años, o con pena pecuniaria, «la destrucción, daño, remoción, alteración o inutilización de un sistema de elaboración de datos o de un soporte informático de almacenamiento de datos» («eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert»).
54. En este sentido, es paradigmática la decisión tomada por el legislador belga, que con la Ley número 34, de 28 noviembre de 2000, ha introducido en el Código penal un nuevo título IX-bis, que recoge las «infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes».
55. Sobre estos fundamentales principios del Derecho penal, véanse, además de los fundamentales trabajos de Bricola (1973, pág. 42 y sig.; y «Art. 25, 2° e 3° comma», en Branca, 1981, pág. 227 y sig.), también Vassalli (1991, pág. 699 y sig.); Donini (1996, pág. 25 y sig.; 2003, «Ragioni e limiti della fondazione del diritto penale sulla Carta costituzionale», en *Alla ricerca di un disegno. Scritti sulle riforme penali in Italia*, Padua, Cedam, pág. 37 y sig.; 1998, «Dogmatica penale e politica criminale a orientamento costituzionalistico. Conoscenza e controllo critico delle scelte di criminalizzazione», *Dei delitti e delle pene,* núm. 3, pág. 37 y sig.); Palazzo (1999); Paliero (1991, pág. 395 y sig.); Mazzacuva (2000, pág. 79 y sig.).

Bibliografía

ANGIONI, F. (1983). *Contenuto e funzioni del concetto di bene giuridico*. Milán: Giuffrè.

ANGIONI, F. (1994). *Il pericolo concreto come elemento della fattispecie: la struttura oggettiva*. Milán: Giuffrè. 2.ª ed.

ARDIZZONE, S. (1984). *I reati aggravati dall'evento*. Milán: Giuffrè.

BONDI, A. (1994). «"L'esclusività" di Rengier. Contributo alla critica dei reati aggravati dall'evento». *Rivista italiana di diritto e procedura penale*. Pág. 1460 y sig.

BONDI, A. (1999). *I reati aggravati dall'evento tra ieri e domani*. Nápoles: Edizioni Scientifiche italiane.

BRANCA, G. (1981). *Commentario della Costituzione: Rapporti civili*. Bolonia: Zanichelli.

BRICOLA, F. (1962). «Danneggiamento (Diritto penale)», voz en *Enciclopedia del diritto*. Milan: Giuffrè.

BRICOLA, F. (1973). «Teoria generale del reato». *Nss. dig. it*. Vol. XIX, pág. 1 y sig.

CONCAS, L. (1967). «Delitti dolosi aggravati da un evento non voluto e tentativo». *Rivista italiana di diritto e procedura penale*. Pág. 809 y sig.

DELITALA, G. (1930). *Il «fatto» nella teoria generale del reato*. Padua: Cedam.

DONINI, M. (1996). *Teoria del reato. Una introduzione*. Padua: Cedam.

DONINI, M. (1998). «Dogmatica penale e politica criminale a orientamento costituzionalistico. Conoscenza e controllo critico delle scelte di criminalizzazione». *Dei delitti e delle pene*. Núm. 3, pág. 37 y sig.

DONINI, M. (2003). *Alla ricerca di un disegno. Scritti sulle riforme penali in Italia*. Padua: Cedam.

DREHER, E.; LACKNER, K.; KÜHL, K. (2011). *Strafgesetzbuch Kommentar*. Múnich: Beck Verlag. 27ª edición.

FIANDACA, G.; MUSCO, E. (2007). *Diritto penale, Parte speciale*. Bolonia: Zanichelli. 5.ª ed. Vol. II, tomo II.

FIANDACA, G.; MUSCO, E. (2012). *Diritto penale, Parte generale*. Bolonia: Zanichelli. 6.ª ed.

FISCHER, T. (2010). *Strafgesetzbuch und Nebengesetze*. Múnich: Beck Verlag. 57.ª ed.

GALLO, E. (1966). *Il delitto di attentato nella teoria generale del reato*. Milán: Giuffrè.

GALLO, E. (1987). «Attentato», voz en *Digesto discipline penalistiche*. Vol. I, pág. 345 y sig.

GALLO, E. (1990). «Delitti aggravati dall'evento e delitti di attentato». *Giurisprudenza italiana*. Pág. 409 y sig.

GALLO, M. (1949). «Sulla distinzione tra figura autonoma e figura circostanziata». *Rivista italiana di diritto e procedura penale*. Pág. 560 y sig.

GRASSO, G. (1986). «L'anticipazione della tutela penale: i reati di pericolo e i reati di attentato». *Rivista italiana di diritto e procedura penale*. Pág. 689 y sig.

GROSSO, C. F. (1963). «Struttura e sistematica dei cd. "delitti aggravati dall'evento"». *Rivista italiana di diritto e procedura penale*. Pág. 442 y sig.

GUERRINI, R. (1988). *Elementi costitutivi e circostanze del reato*. Milán: Giuffrè.

HILGENDORF, E. (1996). «Grundfälle zum Computerstrafrecht». *Juristische Schulung*. Pág. 892.

HILGENDORF, E.; FRANK, T.; VALERIUS, B. (2005). *Computer und Internetstrafrecht*. Berlín / Heildelberg: Springer.

HOYER, E. (2009). «§ 303a StGB». En: H.-J. RUDOLPHI, E. HORN, H.-L. GÜNTHER, E. SAMSON (ed.). *Systematischer Kommentar zum Strafgesetzbuch*. Múnich: Heymann. Pág. 27, 3.

MANTOVANI. F. (2009). *Diritto penale, Parte speciale*. Padua: Cedam. 3.ª ed. Vol. II.

MARINUCCI, G. (1983). «Fatto e scriminanti. Note dommatiche e politico-criminali». *Rivista italiana di diritto e procedura penale*. Pág. 1237 y sig.

MARINUCCI, G.; DOLCINI, E. (2001). *Corso di diritto penale*. Milán: Giuffrè.

MAZZACUVA, N. (1983). *Il disvalore di evento nell'illecito penale*. Milán: Giuffrè.

MAZZACUVA, N. (2000). «Diritto penale e Costituzione». En: G. INSOLERA, N. MAZZACUVA, M. PAVARINI, M. ZANOTTI (ed.). *Introduzione al sistema penale*. Turín: Giappichelli. Vol. I, pág. 79 y sig.

MELCHIONDA, A. (2000). *Le circostanze del reato*. Padua: Cedam.

MEUNIER, C. (2001). «La loi du 28 novembre 2000 relative à la criminalité informatique ou le droit pénal et la procédure pénale à l'ère numérique». *Revue de droit pénal et de criminologie*. Pág. 630 y sig.

MIR PUIG, S. (2009). «El principio de proporcionalidad como fundamento constitucional del Derecho penal». En: J. C. CARBONELL MATEU, J. L. GONZÁLEZ CUSSAC, E. ORTS BERENGUER (coord.). *Constitución, derechos fundamentales y sistema penal*. Valencia: Tirant lo Blanch. Pág. 1357 y sig.

MUCCIARELLI, F. (1996). «Commento agli art. 1, 2, 4 e 10 l. 1993 n. 547». *Legislazione penale*. Pág. 57 y sig.

NUVOLONE, P. (1975). *Il sistema del diritto penale*. Padua: Cedam.

PADOVANI, T. (1984). «La tipicità inafferrabile. Problemi di struttura obiettiva delle fattispecie di attentato contro la personalità dello Stato». En: VV. AA. *Il delitto politico dalla fine dell'ottocento ai giorni nostri*. Roma: Sapere 2000. Pág. 169 y sig.

PADOVANI, T. (2008). *Diritto penale*. Milán: Giuffrè. 9.ª ed.

PAGLIARO, A. (1960). *Il fatto di reato*. Palermo: Priulla.

PALAZZO, C. F. (1992). «I confini della tutela penale: selezione dei beni e criteri di criminalizzazione». *Rivista italiana di diritto e procedura penale*. Pág. 453 y sig.

PALAZZO, C. F. (1999). *Introduzione ai principi di diritto penale*. Turín: Giappichelli.

PALIERO, E. (1991). «Il principio di effettività nel diritto penale: profili politico-criminali». En: M. PISANI (ed.). *Studi in memoria di Pietro Nuvolone*. Milán: Giuffrè. Vol. I, pág. 395 y sig.

PARODI GIUSINO, M. (1990). *I reati di pericolo tra dogmatica e politica criminale*. Milán: Giuffrè.

PECORELLA, C. (2006a). «Commento all'art. 615-ter c.p.». En: E. DOLCINI, G. MARINUCCI (ed.). *Codice penale commentato*. Milán: Giuffrè. 2.ª ed. Pág. 4330 y sig.

PECORELLA, C. (2006b). *Il diritto penale dell'informatica*. Padua: Cedam. 2.ª ed.

PECORELLA, C. (2011). «La riforma dei danneggiamenti informatici ad opera della l. n. 48/2008». En: F. RUGGIERI, L. PICOTTI (ed.). *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*. Turín: Giappichelli. Pág. 148 y sig.

PETROCELLI, B. (1955). *Il delitto tentato*. Padua: Cedam.

PICA, G. (1999). *Diritto penale delle nuove technologie*. Turín: Giappichelli.

PICOTTI, L. (2000). «Reati informatici». voz en *Enciclopedia Giuridica*, Vol. de actualización VIII, Roma: Treccani, pág. 8 y sig.

PICOTTI, L. (2004). «Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati». En: *Il diritto penale dell'informatica nell'epoca di Internet*. Padua: Cedam. Pág. 58 y sig.

PICOTTI, L. (2008a). «La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale». *Diritto penale e processo*. Pág. 713.

PICOTTI, L. (2008b). «Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo». *Diritto dell'Internet*. Núm. 5, pág. 437 y sig.

PREZIOSI, S. (2000). *La fattispecie qualificata*. Padua: Cedam.

PULITANÒ, D. (1967). «Illiceità espressa e illiceità speciale». *Rivista italiana di diritto e procedura penale*. Pág. 65 y sig.

RINALDI, R. (1996). «Commento all'art. 9, l. 23 dicembre 1993, n. 547». *Legislazione penale*. Pág. 134 y sig.

ROMANO, M. (2004). *Commentario sistematico del codice penale*, I, sub art. 56 c.p. Milán: Giuffrè. 3.ª ed.

ROXIN (2006). *Strafrecht, AT*. Múnich: Beck Verlag, 4.ª ed., vol. I, pág. 423-426, mar.147-152.

SALVADORI, I. (2008). «Hacking, cracking e nuove forme di attacco ai sistemi di informazione. Profili di diritto penale e prospettive de jure condendo». *Cyberspazio e diritto*. Núm. 3, pág. 354 y sig.

SALVADORI I. (2012). «Il "microsistema" normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante». *Rivista italiana di diritto e procedura penale*, pág. 204 y sig.

SALVADORI I. (2011), «Los nuevos delitos informáticos introducidos en el Código Penal español con la Ley Orgánica 5/2010. Perspectiva de derecho comparado». *Anuario de Derecho Penal y Ciencias Penales*. vol. LXIV, pág. 221 y sig.

SARZANA, C. (2008). «La legge di ratifica della Convenzione di Budapest: una "gatta" legislativa frettolosa». *Diritto penale e processo*. Núm. 12, pág. 1562 y sig.

SCOPINARO, L. (2007). *Internet e reati contro il patrimonio*. Turín: Giappichelli.

SIEBER, U. (1986). *The International Handbook on Computer Crime. Computer related Economic Crime and the Infringements of Privacy*. Chichester: Wiley.

STREE, W.; HECKER, B. (2010). «§ 303a StGB». En: A. SCHÖNKE, H. SCHRÖDER (ed.). *Strafgesetzbuch Kommentar*. Múnich: Beck Verlag. 28.ª ed. Pág. 2664 y sig.

TAGLIARINI, F. (1979). *I delitti aggravati dall'evento. Profili storici e prospettive di riforma*. Padua: Cedam.

VASSALLI, G. (1975). «Concorso tra circostanze eterogenee e "reati aggravati dall'evento"». *Rivista italiana di diritto e procedura penale*. Pág. 3 y sig.

VASSALLI, G. (1991). «I principi generali del diritto nell´esperienza penalistica». *Rivista italiana di diritto e procedura penale*. Pág. 699 y sig.

VV. AA. (2006). *Diritto penale. Lineamenti di parte speciale*. Bolonia: Zanichelli. 4.ª ed.

WOHLERS, W. (2000). *Deliktstypen des Präventionsstrafrechts - zur Dogmatik «moderner» Gefährdungsdelikte*. Berlín: Duncker und Humblot.

WOLFF, H. (2010). «§ 303a StGB». En: H.-W. LAUFHÜTTE, R. RISSING-VAN SAAN, K. TIEDEMANN (ed.). *Leipziger Kommentar, StGB*. Berlín: De Gruyter. 12.ª ed., vol. 6. Pág. 403.

ZACZYK, R. (2010). «§ 303a StGB». En: U. KINDHÄUSER (ed.). *Strafgesetzbuch*. Baden-Baden: Nomos. 4ª ed. Pág. 2481, marg. 7.

ZIESCHANG, F. (1998). *Gefährdungsdelikte*. Berlín: Dunckler und Humblot.

ZUCCALÁ, G. (1977). «Profili del delitto di attentato». *Rivista italiana diritto procedura penale*. Pág. 1225 y sig.

Cita recomendada

SALVADORI, Ivan (2013). «La regulación de los daños informáticos en el código penal italiano». En: María José PIFARRÉ (coord.) «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política*. Número 16, pág. 44-60. UOC. [Fecha de consulta: dd/mm/aa]
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-salvadori/n16-salvadori-es>
DOI: http://10.7238/idp.v0i16.1831

Sobre el autor

Ivan Salvadori
ivansalvadori@gmail.com
Doctor europeo en Derecho penal económico e informático, investigador posdoctoral
en la Università di Verona (Italia), profesor de Derecho penal en la Universidad de Barcelona

www.ivansalvadori.net
Universidad de Barcelona
Departamento de Derecho Penal y Ciencias Penales
Diagonal Nord, Facultad de Derecho
Principal, pl. 4.a
Av. Diagonal, 684
08034 BARCELONA