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

IDP Número 16 (Junio 2013)

MONOGRÁFICO

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

UOC
Universitat Oberta de Catalunya

ISSN 1699-8154
http://idp.uoc.edu

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»

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

www.uoc.edu/idp

INTRODUCCIÓN

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

María José Pifarré
Profesora de los Estudios de Derecho y Ciencia Política (UOC)

Fecha de presentación: junio de 2013

Internet y, de manera muy especial, las redes sociales conforman un nuevo contexto social caracterizado, entre otras cosas, porque el alcance temporal y espacial de las comunicaciones a través de ellos crea proximidades «virtuales» antaño imposibles que han cambiado el modo en que nos relacionamos en sociedad. En este contexto, con sus particularidades y especificidades, han surgido conductas hasta ahora inéditas y ha tenido lugar una importante mutación de las convenciones sociales. La rapidez con que los comportamientos sociales cambian a causa de Internet, o con que nacen nuevas realidades en su seno, tiene pocos precedentes.

Es evidente que las tecnologías de la información y la comunicación han simplificado extremadamente nuestra vida. Ya no hace falta desplazarse para comprar, ir al banco o realizar trámites con las administraciones públicas, el correo tradicional se ha visto superado en eficacia por la comunicación a través del correo electrónico y las redes sociales, la búsqueda de datos se ha vuelto instantánea sin necesidad de acudir directamente a las fuentes «reales». El ahorro de tiempo es indiscutible. Una parte importante de nuestras vidas transcurre en Internet.

Esta realidad ha hecho que nuestra dependencia de los medios electrónicos que nos dan acceso a la red sea de una envergadura tal que si nos vemos privados de la posibilidad de utilizarlos los daños ocasionados pueden ser muy graves tanto en el ámbito de la vida privada como en el de las empresas y entidades, ya que la mayor parte de la organización e información pasa a través de ellos. De ahí que, históricamente, la primera reacción del Derecho penal fuera la tipificación de los delitos informáticos, centrándose en aquellos que dañan los datos y los sistemas informáticos. Sin embargo, mucho ha llovido desde sus primeras proposiciones, y el tiempo ha hecho necesarios cambios sustanciales. A su análisis y al de su nueva regulación en Italia, aunque comparándola con el resto de las legislaciones europeas, incluida la española, se dedica el primer artículo de los propuestos en este dossier, que corre a cargo de Ivan Salvadori. El autor examina estos delitos, de difícil encaje en los delitos tradicionales de daños a las cosas, que han requerido de la creación de nuevos tipos penales al amparo de una legislación internacional que ha ido cambiado progresivamente.

Paralelamente, el desplazamiento de la normal actividad social a la red ha conllevado el desplazamiento del delito tradicional al delito en la red, que es donde ahora se desarrolla la vida y en consecuencia donde hay oportunidad para el delito. Para adaptarse a la nueva realidad, el delito ha debido transformarse adoptando nuevas formas que lo hagan eficaz en este medio. Se ha generado un conjunto de nuevos comportamientos delictivos

para que nada cambie, es decir, para poder conseguir los mismos objetivos que antes, pero a través de los nuevos medios. Pero también se han generado otros totalmente nuevos, que antes no se daban. Por otra parte, una de las consecuencias más importantes de este traslado de la vida cotidiana a Internet es la enorme cantidad de destinatarios potenciales de las acciones delictivas, que alcanza prácticamente el mundo entero, y que las convierte, por el mero hecho de que se cometan en la red, en más peligrosas y lesivas.

Un ejemplo de nuevos comportamientos surgidos a raíz de esta «emigración» a Internet nos lo da el perfil criminológico del acosador, que en general es distinto cuando su actividad de acoso se desarrolla solo en la red. Mientras que en el mundo real el acosador se enfrenta a su víctima principalmente de manera directa y por tanto se suele tratar de una persona con un perfil fuerte, la persona que solo acosa a través de la red suele obedecer a un patrón más apocado, que sería incapaz de realizar la misma conducta en el mundo real, y se ampara en el anonimato y la distancia que le proporciona la red. El segundo artículo del dossier, a cargo de Fernando Miró, parte de esta realidad. Parte del análisis criminológico del ciberacoso para seguir con el análisis del tratamiento que le ha dado la jurisprudencia en España, y por último perfila los tipos penales tradicionales con los que se puede contar para su persecución teniendo en cuenta que no existe un tipo específico unitario para esta realidad y que su castigo pasa a través de tipos penales tradicionales.

Sin embargo, el cambio profundo más reciente lo constituye, sin duda alguna, el desarrollo de las redes sociales. Su uso masivo ha comportado, entre muchas otras consecuencias positivas y negativas, una innegable relajación de la autotutela de la intimidad de una gran parte de la sociedad, que utiliza la red como una vitrina permanente de su vida y su actividad tanto privada como pública, sin acabar de comprender ni controlar el alcance de lo que vierte en ella. La entrada de los menores en este mundo constituye un ulterior problema de grandes dimensiones, porque son sujetos todavía no enteramente capaces de comprender el alcance actual y futuro de sus actos, lo que plantea el interrogante de cómo afrontar la natural desprotección de los menores en Internet, entorno que a menudo sus padres y educadores conocen de manera insuficiente y en el que no son capaces de protegerles ni de enseñarles a autoprotegerse, creando así un espacio de riesgo de especial relevancia en un medio del que tanto podrían beneficiarse. Este tipo de comportamientos está exponiendo al ciudadano a convertirse, no solo en víctima, sino también en autor de muchos delitos cometidos en ese ámbito. De este tema se ocupa el tercer trabajo del dossier, a cargo de Lorenzo Picotti, que analiza la suerte que corren los derechos fundamentales en las redes sociales y cómo el Derecho penal trata de protegerlos, de manera que ofrece al lector algunos de los argumentos de más actualidad para tratar ciertos comportamientos peligrosos que llevan camino de consolidarse en el uso de las redes sociales.

Estos últimos son solo algunos de los varios debates que se han abierto en la sociedad acerca de la bondad, aceptabilidad, oportunidad e incluso moralidad de muchas de las conductas realizadas en el ámbito de las nuevas tecnologías. También, naturalmente, acerca de su legalidad.

En este debate se enmarcan los artículos de este dossier monográfico, que tratan aspectos bien distintos de las relaciones entre Internet y redes sociales con el Derecho penal, desde puntos de vista diversos y con metodología diferente. Con esta selección se ha pretendido que cada aportación valore un aspecto distinto de esta múltiple realidad, pero sobre todo se le ha querido dotar de una importante valencia internacional en el convencimiento de que la transnacionalidad de estos fenómenos exige abrir una vía hacia la fundamental dimensión internacional que debe asumir la reflexión y búsqueda de posibles soluciones, principalmente porque Internet no tiene y no entiende de fronteras. Toda solución que no tenga en cuenta este elemento será estéril.

La inevitable globalidad del fenómeno, además, queda patente en el hecho de que en la mayoría de los países de nuestro entorno cultural se han dado normas penales que pretenden seguir las propuestas elaboradas en el seno de la Unión Europea o de los numerosos tratados internacionales en la materia, principalmente impulsados por la ONU. Esta aparente «homogeneidad» que su origen unitario debería imprimir, sin embargo, no hace que la internalización de estas normas se traduzca en la realidad en una uniformidad de tratamiento. Las particularidades culturales y de tradición legislativa de cada Estado han acabado dando formas muy diferentes que es interesante y conveniente estudiar. Conociéndolas seremos capaces también de dirigir una mirada más crítica a nuestro ordenamiento y podrá ayudarnos a encontrar mecanismos de respuesta y solución alternativos, porque conoceremos también los problemas que esas soluciones han planteado en otros países.

Bajo todos estos puntos de vista Internet está ofreciendo uno de los mayores retos a quienes tienen como tarea

reflexionar acerca de los instrumentos penales adecuados para tratarlo, ya sean los investigadores universitarios, el legislador, tanto nacional como europeo e internacional, o los Cuerpos y Fuerzas de Seguridad del Estado, y en estos artículos se pueden encontrar elementos de juicio para esta reflexión. La necesidad de soluciones inmediatas es evidente, y la rapidez con que se suceden los cambios hace difícil una previa reflexión serena. Los poderes públicos tratan de reaccionar ante esta situación con medidas que adoptan de manera urgente, muchas veces con intención de que sean provisionales en tanto la «alarma social» provocada en ciertos sectores siga viva, y todo ello sin que la propia sociedad haya cerrado los distintos debates, o al menos llegado a un consenso suficiente en ellos. Efectivamente, uno de los instrumentos más utilizados por los poderes públicos ante estas «emergencias», porque el ciudadano lo suele percibir como solución inmediata, o al menos como que los poderes públicos toman medidas, es el Derecho penal, que además no comporta la asignación de una partida presupuestaria directa.

Un claro ejemplo de ello es el recientísimo Proyecto de Ley de modificación del Código Penal presentado hace pocos días, este mismo mes de septiembre, cuando aún están frescas las reformas anteriores en materia de ciberdelitos. Algunas de las propuestas que contiene son ya fruto de la maduración de ciertos debates, pero otras constituyen medidas nuevas que será necesario analizar. En este último caso, la legislación penal en la materia que nos ocupa está asumiendo un papel de «concienciador» o «educador» de la sociedad, como lo es el caso de la propuesta tipificación de un delito de creación y mantenimiento de páginas de enlaces para evitar comportamientos lesivos de la propiedad intelectual.

El Proyecto no es más que un ejemplo de la rapidez y profundidad con que se están sucediendo los cambios legislativos en este campo, algunos de los cuales dan respuesta a cuestiones puestas de relieve por los autores del dossier, como la conveniencia o no de una regulación autónoma del *sexting,* o el ciberacoso, tratados por Fernando Miró y Lorenzo Picotti. El Proyecto, ciertamente, propone modificaciones de calado en la materia, como la creación de una circunstancia agravante específica al delito de incitación al odio o a la violencia racial cuando esta se cometa a través de Internet; el castigo de la creación y mantenimiento de páginas de enlaces; la creación de un delito de acoso dentro del capítulo de las coacciones que es perfectamente susceptible de ser cometido a través de Internet, conducta de la que psicólogos y sociólogos están advirtiendo desde hace ya tiempo; la creación de un nuevo delito contra de la intimidad para los casos de *sexting*, que durante el pasado año han trascendido a los medios de comunicación y han creado una importante alarma social (caso de la alcaldesa de Los Yébenes), de manera que se castigarían los casos en que se obtienen imágenes o grabaciones de otra persona dentro de su ámbito íntimo con su consentimiento pero se divulgan contra su voluntad con lo que se vulnera gravemente su intimidad; se sancionaría también el acceso voluntario a pornografía infantil en Internet y a quien en este ámbito contacte con menores con fines sexuales. En este caso, además, prevé una norma de extensión de aplicación de la ley penal española a los delitos contra la libertad e indemnidad sexual de los menores cometidos en Internet siempre que los contenidos en cuestión sean accesibles desde territorio español, independientemente del lugar donde estas actividades tengan su base. Por otra parte, para muchos de estos delitos prevé la retirada de contenidos y la posibilidad de bloqueo del portal de acceso.

Estas propuestas ministeriales, algunas de las cuales dan respuesta a necesidades puestas de relieve en los artículos que forman este dossier, nos dan nuevos motivos para la lectura de estos artículos. Confiamos en que susciten el interés del lector y que contribuyan a la imprescindible discusión y análisis crítico de la normativa penal en materia de Internet y redes sociales tanto de *lege lata* como de *lege ferenda*.

Cita recomendada
PIFARRÉ, María José (2013). «Introducción». En: «Internet y redes sociales: un nuevo contexto para el delito» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política.* Número 16, pág. 40-43. UOC. [Fecha de consulta: dd/mm/aa]
‹http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-pifarre/n16-pifarre-es›
DOI: DOI: 10.7238/idp.v0i16.1985

Sobre la autora

María José Pifarré
mpifarre@uoc.edu
Profesora de los Estudios de Derecho y Ciencia Política (UOC)

Doctora en Derecho penal: Dottore di Ricerca in diritto penale, con mención de excelencia (Università degli Studi di Macerata, Italia, 2008), suficiencia investigadora (Universitat de Barcelona, 1997), Master en Derecho penal y Ciencias penales (Universitat de Barcelona, 1995) y licenciada en Derecho (Universitat de Barcelona, 1990)

http://www.uoc.edu/webs/mpifarre/ES/curriculum/

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

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

Derecho penal, *cyberbullying* y otras formas de acoso (no sexual) en el ciberespacio

Fernando Miró Llinares
Profesor titular de Derecho Penal
Universidad Miguel Hernández de Elche

Fecha de recepción: mayo de 2013
Fecha de aceptación: mayo de 2013
Fecha de publicación: junio de 2013

Resumen
Las redes sociales, en particular, e Internet en general, constituyen hoy en día un nuevo ámbito de desarrollo personal, un nuevo espacio vital en el que cada individuo pasa varias horas al día, se comunica con otros, crea relaciones, y en el que, por tanto, también se cometen ataques contra bienes individuales como el honor, la libertad, la intimidad o la propia dignidad personal. En el presente trabajo se analiza la respuesta del ordenamiento penal español a las distintas formas de acoso no sexual a menores realizado en el ciberespacio. A partir de la descripción y conceptualización de fenómenos como el *cyberbullying*, o los actos individuales de *online harassment*, se analiza la concreta incardinación de las distintas modalidades de acoso, continuado o no, a menores, en los diferentes tipos de la parte especial. Al no existir un precepto penal que regule expresamente la mayoría de estas conductas, y pese a haberse convertido el tipo básico de los delitos contra la integridad moral en el delito de referencia para los tribunales, son varios (amenazas, coacciones, injurias, etc.) los tipos penales que pueden aplicarse en conductas de acoso, generalmente entre iguales, que, como se verá por el amplísimo repertorio jurisprudencial, están comenzando a proliferar en el ciberespacio.

Palabras clave
cibercrimen, ciberacoso, *cyberbullying, online harassment, cyberstalking*

Tema
cibercrimen

Criminal law, cyberbullying and other forms of (non-sexual) harassment in cyberspace

Abstract

Social networks, in particular, and the Internet, in general, now represent a new ambit for personal development, a new life space where people spend hours of their day communicating with others and forming relationships, and where, thus, there are attacks on individuals and their honour, liberty, privacy or personal dignity. This article analyses the response of Spanish criminal law to the different forms of non-sexual harassment of minors in cyberspace. Following the description and conceptualization of phenomena such as cyberbullying or individual acts of online harassment, the article analyses the specific incorporation of different forms of harassment of minors, whether continuous or not, in the different types of the particular part of the law. There is no criminal precept that expressly regulates most of these acts (despite the basic type of crimes against moral integrity having been made the benchmark crime for the courts). The types of crime that can be applied to these harassing behaviours – generally among peers – which are starting to proliferate in cyberspace are varied (threat, coercion, slander, etc.), as can be seen in the wide range of jurisprudence.

Keywords

cybercrime, cyberbullying, online harassment, cyberstalking

Subject

cybercrime

1. Tipificar expresamente o no hacerlo, «he ahí la cuestión»

La doctrina penal ha criticado en reiteradas ocasiones la tendencia del legislador a regular expresamente nuevos tipos penales que, sin embargo, venían a sancionar conductas que ya merecían un reproche penal anterior por medio de otros preceptos. Esto sucede especialmente con la aparición en la sociedad de nuevos conceptos correspondientes a realidades que ya existían, y que incluso podían estar reguladas penalmente, pero que no eran conocidas o, siéndolo, apenas estaban desvaloradas socialmente. Ante la aceptación social de nuevos términos, apenas conocidos para una mayoría de los ciudadanos en un determinado momento histórico, como el *acoso sexual*, el *mobbing*, el *bullying* o el *stalking*, surge, antes incluso que la duda de si tales conductas merecen un reproche penal o si ya lo tienen, la tentación de crear un tipo penal específico que cumpla con la función simbólica que, en las últimas décadas, protagoniza el sentido de la incriminación penal. Al fin y al cabo, con la tipificación se logran los efectos deseados por el legislador: si la conducta no está recogida de forma íntegra en la regulación actual, se comunica a la sociedad el mensaje de que ahora lo está y, en el caso de que sí lo estuviera, cuando menos se refuerza la idea de que ese hecho se castiga y, sobre todo, de que el Estado interviene de forma eficaz frente a los problemas sociales existentes. Se olvidan, sin embargo, los múltiples problemas técnico-jurídicos que conlleva la creación *ex novo* de un precepto para la incriminación de conductas que ya podían sancionarse por otros.

Cuando, por el contrario, surge a la luz pública un fenómeno criminal nuevo o que, habiendo existido durante muchos años, es ahora cuando nace acerca de él una preocupación social grave, y no existe un precepto penal específico que lo englobe, los problemas son otros. El principal estriba en la determinación de los preceptos penales adecuados para responder a las distintas conductas de nueva factura. Y este se acrecienta cuando la fenomenología de comportamientos es extremadamente variada, no solo en lo cuantitativo sino también en lo cualitativo.

Esto es lo que ha sucedido en los últimos años con la respuesta penal a los distintos actos de acoso a menores en el ciberespacio que suelen identificarse conceptualmente, y no siempre de forma adecuada, con los términos –que no debieran entenderse como sinónimos– de *ciberacoso a menores* o de *cyberbullying*. Por una parte no hay un precepto penal titulado de ninguna de estas dos formas ni que se incorporase al texto punitivo tras la aparición de este tipo de fenómenos y con propósito de regularlos. Por otra, y quizás por la imprecisión que suele dar la inexistencia de un concepto jurídico expreso, bajo la vaguedad de los términos *ciberacoso* y *ciberbullying* cabe una infinidad de conductas realizadas sobre menores cuya gravedad difiere enormemente entre ellas. De hecho, esto ya le sucede a los propios conceptos de *acoso* o de *bullying*, que por no tener una regulación penal específica no solo no hay un consenso claro sobre su alcance, sino que engloban conductas de lesividad para los intereses en juego muy dispares entre sí.

El presente trabajo aborda el análisis de la respuesta del Código penal a las distintas variedades de acoso no sexual a menores realizado en el ciberespacio. El objeto de estudio no es, por tanto, solo el *cyberbullying*, sino también el acoso de mayores a menores realizado a través de Internet y tanto si se realiza de forma continuada y sistemática como si se limita a la realización de acciones individuales de acoso que pueden enmarcarse en delitos contra el honor, la libertad o similares. Por ello, y previamente al análisis jurisprudencial y doctrinal de cómo responden las leyes penales a las distintas conductas, trataré de identificar estas partiendo del propio alcance que desde la psicología y la criminología se ha dado al término *cyberbullying*. Así no solo podremos identificar las distintas conductas sino también –lo que debe ser más importante para la posterior fijación del merecido reproche penal de cada una de ellas– su muy diferente gravedad para la dignidad, libertad, honor y otros bienes personalísimos de los menores que se ven puestos en peligro en la actualidad también en ese ámbito de intercomunicación personal que es el ciberespacio.

2. Fenomenología: *cyberbullying*, *online harassment* y otras nomenclaturas referidas al acoso a menores en el ciberespacio

Desde que se empezara a estudiar el fenómeno del *bullying* en los años setenta,[1] se ha discutido acerca de la idoneidad de cada uno de los elementos que deben formar parte de la definición,[2] desde quién debe protagonizar la agresión (un grupo de compañeros o, por el contrario, puede ser suficiente con que el daño lo ejerza una sola persona) hasta la inclusión de las distintas formas de agresión (física, psicológica o verbal), pasando por la necesidad de que exista un desequilibrio de poder real o imaginario entre agresor y víctima, la repetición del daño durante un periodo prolongado, la intencionalidad del agresor, la autopercepción de la víctima y los efectos que estas conductas tienen sobre las personas que participan.[3] Actualmente puede decirse que la definición más aceptada es la de Dann Olweus, quien entiende que hay victimización por *bullying* cuando «un alumno está expuesto repetidamente y a lo largo del tiempo a acciones negativas de otro o un grupo de estudiantes».[4] Esta definición incluye los tres elementos que caracterizan el *bullying*: debe existir la intencionalidad de agredir a la víctima, la agresión debe ser repetida en el tiempo y debe existir un desequilibrio de poder entre agresor y víctima.[5] Esta discusión sobre el contenido y alcance del *bullying* afecta también al concepto de *cyberbullying*, definido por Patchin e Hinduja como el «daño intencional y repetido infligido a través del medio del texto electrónico».[6] Por su parte, Smith et al., además de los elementos intencionalidad, repetición y uso de las TIC, añaden el desequilibrio de poder, definiéndolo como «una acción agresiva e intencional, desarrollada por un grupo o un individuo, usando formas electrónicas de contacto, repetidas veces a lo largo del tiempo contra una víctima que no puede defenderse fácilmente».[7] En lo que sí coincide la doctrina es en la multiplicidad de formas que

1. El primer estudio publicado data de 1969 y fue elaborado por el psiquiatra noruego Peter Paul Heinemann, quien describió el acoso al que era sometido un estudiante por un grupo de compañeros en el patio del colegio.
2. D. P. Farrington, 1993.
3. R. Ortega, R. del Rey, J. Mora-Merchán, 2001.
4. D. Olweus, 1994.
5. J. Calmaestra Villén, 2011.
6. J. W. Patchin, S. Hinduja, 2006.
7. P. K. Smith et al., 2008.

puede adoptar el maltrato, incluyéndose acciones como atormentar, amenazar, acosar, humillar, avergonzar, etc.,[8] conductas que, como puede intuirse, no siempre van a tener encaje en los preceptos tradicionales del Código penal.

Este entendimiento del *bullying* incide en la comprensión del *cyberbullying*, que puede entenderse como el abuso de poder continuado de un menor sobre otro realizado por medio del uso de las TIC. El *cyberbullying* seguiría caracterizándose por conductas centradas en atormentar, amenazar, humillar, hostigar o molestar al menor, pero estas ya no tienen como ámbito la escuela ni ningún otro espacio físico, sino el ciberespacio, lo cual, según el parecer de la mayoría de los autores que han analizado el fenómeno, también conlleva que cambien los autores, las causas y las consecuencias de esta forma de acoso.[9] En este sentido entiende Calmaestra que para hablar de *cyberbullying* debemos seguir exigiendo los caracteres de «intencionalidad, repetición y desequilibrio de poder», si bien Internet añade matices diferenciadores a esta forma de *bullying*: el anonimato, el carácter público de la agresión o el que la misma se pueda cometer sin restricciones espaciales ni temporales.[10] Hay que tener en cuenta, además, que en ocasiones el *cyberbullying* puede constituir un acoso autónomo realizado exclusivamente en el ciberespacio, pero en otras es una extensión del acoso realizado en el ámbito escolar, utilizándose Internet para reforzar el *bullying* ya emprendido en el horario escolar.[11]

El *cyberbullying*, pues, debe diferenciarse conceptualmente de dos fenómenos que también han adquirido significación en los últimos años. El primero es el *cyberstalking*,[12] que englobaría las conductas de acoso u hostigamiento continuado a adultos en el ciberespacio, y que, precisamente por la edad del sujeto pasivo del ataque, no es objeto de interés en este trabajo. El segundo es el del *online harassment*, también denominado *cyberharassment*, que suele emplearse para referirse a actos concretos, y no continuados, de *bullying* o *stalking* en el ciberespacio.[13] El *cyberharassment*, por tanto, incluiría todas las conductas de *cyberbullying* (y también de *cyberstalking* cuando se realiza sobre un adulto) cuando no son realizadas de forma continuada por el mismo sujeto o sujetos sobre la misma víctima, entre las cuales las más habituales son las siguientes: el envío de mensajes amenazantes o abusivos a través del correo electrónico, la mensajería instantánea o el chat; la publicación de información falsa sobre la víctima; la suplantación de identidad con fin de burla, de obtener información o de dañar de cualquier modo al sujeto; la intimidación o coacción a través de comunicación escrita o verbal por medio de Internet; el insulto o calumnia leve y grave; la incitación a otras personas al acoso o a proferir amenazas o a agredir a la víctima; el envío de software malicioso o de material pornográfico u ofensivo para dañar a la víctima, etc.[14]

Los menores, por tanto, pueden sufrir, por parte de compañeros o de adultos, una amplia gama de ataques que pueden afectar a su honor, intimidad, libertad o dignidad. Para valorar la adecuada respuesta a los mismos, dado que no existe un tipo penal que delimite expresamente qué actos de *cyberbullying* y cuáles de las conductas de *cyberharassment* merecen respuesta penal, habrá que atender a los distintos bienes jurídicos afectados por los ataques. Pero también habrá que tener en cuenta el carácter continuado de la agresión, que es lo que distingue al *cyberbullying* del *online harassment* a partir del argumento del mayor daño psicológico que produce en el menor el hostigamiento repetido, así como la gravedad extrema que algunos actos individualizados pueden entrañar.[15] Esto es especialmente importante en el ciberespacio, que tiene la capacidad de

8. J. Pardo, 2010.
9. J. J. Marco, 2010.
10. J. Calmaestra, *op. cit.*, pág. 104 y ss.
11. M. A. Hernández e I. M. Solano, 2007.
12. El *cyberstalking* ha sido definido como el uso de Internet u otra tecnología de comunicación para hostigar, perseguir o amenazar a alguien (S. Basu, R. Jones, 2007). Hace referencia a la modalidad *online* de *stalking*, término que surgió en los años 90 tras la muerte de dos famosas a manos de personas que las habían acosado y perseguido durante un tiempo (A. Smith, 2009). En la literatura se distinguen dos formas de definir el concepto *cyberstalking* (F. Miró, 2012): por un lado, los que consideran que el *cyberstalking* cumple los requisitos del *stalking* pero en el ciberespacio, como la que explican M. Pathé y P. E. Mullen (1997), que entienden que son los comportamientos en los que un individuo inflige a otro intrusiones o comunicaciones repetidas y no deseadas; y, por otro, los que prefieren definirlo como una suma de actos de *cyberharassment* (P. Bocij, L. McFarlane, 2002; o B. Henson 2010).
13. F. Miró, *op. cit.*, pág. 91.
14. P. Bocij, 2003.
15. D. Olweus, 1993.

hacer perenne lo que en el espacio físico es caduco,[1] y de convertir una broma en una humillación perpetua.[2]

3. Tratamiento penal del ciberacoso a menores

3.1. Introducción

Ya hemos afirmado que el hecho de que el Código penal no contenga una regulación expresa del *cyberbullying* o el *cyberharassment* no supone un obstáculo a la hora de castigar muchos de los ataques que los menores pueden sufrir a través del ciberespacio. Como resulta lógico, la jurisprudencia ha reconducido a distintos tipos penales muchas de las conductas que, con poca precisión, podríamos denominar de «acoso a menores a través de Internet». Y lo ha hecho, como no podría ser de otra forma, a partir de los distintos bienes jurídicos de los menores dañados o puestos en riesgo por los distintos ciberataques. El honor, la libertad, la intimidad, entre otros bienes de los menores que pueden ser afectados, delimitarán la concreta respuesta jurídica. Así, el que, conforme a la conceptualización criminológica, determinados comportamientos puedan definirse como *cyberbullying* o como actos de *cyberharassment*, no influirá, en principio, en que exista una respuesta penal o no a los mismos. Será la afectación a los distintos intereses recogidos en el Código penal lo que delimitará la gravedad de la sanción penal.

La entrada en juego, sin embargo, entre los intereses que pueden ser afectados por las conductas que merecen nuestra atención, del bien jurídico «integridad moral» conlleva que muchas de las conductas de *cyberbullying*, esto es, en las que el abuso de poder es continuado, se hayan reconducido a estos tipos penales. Realizaré, por tanto, el análisis diferenciando, en coherencia con la descripción fenomenológica previa, entre la calificación jurídica de los actos de acoso continuado y la que debe realizarse en el caso de los distintos actos concretos de acoso que pueden afectar a otros bienes jurídicos distintos a la integridad moral.

3.2. La punición del acoso continuado a menores a través de los delitos contra la integridad moral

Aunque la doctrina apenas se ha ocupado hasta el momento de esta fenomenología de cibercrímenes, son muchos los casos de acoso continuado a menores en el ciberespacio enjuiciados por los tribunales. Especialmente conductas de *cyberbullying*, es decir, también perpetradas por menores. Y puede decirse que los tribunales, de forma mayoritaria, acuden a los delitos contra la integridad moral para sancionar este tipo de cibercrímenes sociales. Siguen, en este sentido, idéntico criterio al generalmente aceptado para la calificación del *bullying* tradicional.[18] Es el bien jurídico integridad moral el que, cuando hay un acoso de estas características realizado de forma permanente o continuada en el tiempo, se verá afectado y dará lugar, por tanto, a la aplicación del art. 173 CP. Así lo establece con claridad meridiana la SAP de Ávila 146/2008, de 20 de octubre, que añade que el tipo básico de los delitos contra la integridad moral se aplicará en concurso con los correspondientes tipos penales «de lesiones, amenazas o coacciones, incluyendo cualesquiera de las infracciones previstas en los arts. 617 y 620 CP».[19]

16. F. Miró, 2011.
17. H. Vandebosch, K. van Cleemput, 2009; J. Calmaestra, *op. cit.*, pág. 115.
18. En cuanto a la calificación jurídica del *bullying*, es paradigmática la resolución final del denominado caso Jokin (sentencia del Juzgado de Menores n.º 1 de San Sebastián, n.º 86/2005, de 12 mayo, que fue recurrida ante la AP de Guipúzcoa, resolviendo esta en sentencia n.º 178/2005, de 15 julio). Otros casos de *bullying* tratados recientemente por la jurisprudencia española son, entre otros, el enjuiciado en la SAP de Castellón, n.º 32/2010, de 2 de febrero, en la que también se condena por un delito contra la integridad moral; también en la SAP de Córdoba n.º 78/2008, de 4 de abril; la SAP de A Coruña n.º 459/2008, de 6 de noviembre; la SAP de Castellón n.º 159/2007, de 31 de julio; la SAP de Ávila, n.º 37/2006, de 22 de febrero, y la SAP de Castellón n.º 386/2007, de 3 de julio, en la que además se impone a las autoras una falta de injurias del art. 620.2 por insultar a la víctima. Aunque también se han resuelto en ocasiones los casos de *bullying* imputando la falta de amenazas y vejaciones, como ocurre en la SAP de Barcelona n.º 427/2009, de 8 de mayo, y en la SAP de Ávila n.º 146/2008, de 20 de octubre, en la que se precisa que no se considera probado que la conducta del acusado «fuera constante y repetitiva». Estima en este último caso el juzgador que la actitud del menor, aun siendo un episodio de vejación reiterado, no reviste el carácter de sistemático y diario, de modo que haya llegado a producir una «quiebra moral» en la víctima, ni la nota de gravedad que exige el tipo.
19. En el mismo sentido, también la SAP de Castellón n.º 159/2007, de 31 de julio.

Conductas, por tanto, como la publicación en un portal web de fotos de una menor en situaciones comprometidas, mostrando sus prendas íntimas, ofreciendo, además, a los visitantes de la página la posibilidad de que pudiesen valorar las fotografías exhibidas y efectuar los comentarios que quisieran otorgándoles puntuaciones, todo lo cual fue divulgado por el propio acusado entre el resto de los escolares y compañeros, convirtiéndolos en públicos y notorios, con la consiguiente humillación de la menor, han dado lugar a la aplicación del art. 173 CP.[20] Y también otras, de aparente menor entidad, como la utilización de redes sociales, en este caso Tuenti, para insultar de forma constante a la víctima.[21] Y es que son muchas las resoluciones que exigen una prolongación del acoso en el tiempo para entender la existencia de una afectación suficiente de la integridad moral.[22] Reiteración que, sin embargo, puede no exigirse en el caso de que la entidad del ataque sea tal que, pese a realizarse en una única ocasión, conlleve ya una suficiente afectación a la integridad moral de la víctima. Así lo han interpretado algunas resoluciones, como la SAP de Valencia n.º 488/2009, de 10 de septiembre, que enjuicia un conflicto que tiene su origen en una conducta anterior de *sexting*,[23] en el que la propia víctima consintió la grabación de un vídeo a un amigo que posteriormente lo difundió en Internet e informó de ello a sus compañeros con la intención de humillarla. Señala la resolución, para fundamentar la aplicación del delito del art. 173.1 y no la simple falta de vejaciones, que «no es necesario, como se apunta en alguno de los recursos, que se trate de una pluralidad de actos o exista una continuidad o persistencia en el tiempo. Basta con una sola acción que tenga la suficiente gravedad como para integrar los demás elementos del tipo, el ánimo de humillar y el efectivo padecimiento. En este caso y aunque la acción fuera una sola, sus efectos perduraron con la progresiva difusión de las imágenes y con ella, el sufrimiento de la víctima», concluyendo finalmente que los hechos probados tienen una «entidad suficiente» como para aplicar el delito del art. 173.[24] Y en sentido similar podríamos citar la SAP de Cádiz n.º 23/2011, de 26 de enero, enjuiciando la conducta de un menor que abordó a otro menor con minusvalía psíquica obligándole a correr cuesta arriba con los cordones de las zapatillas atados y grabándolo con el teléfono para colgarlo en YouTube. La resolución se refiere a la jurisprudencia del TS[25] conforme a la cual las conductas no graves exigen reiteración para ser sancionadas por este precepto y señala que para que una conducta sea punible por este tipo, o bien deberá ser habitual o bien deberá existir un riesgo para la integridad moral de la víctima.

Sin entrar en una valoración específica de las citadas resoluciones, lo cierto es que anticipan una línea interpretativa sobre la entidad lesiva de la dignidad de algunos ataques en el ciberespacio especialmente acertada. Como ya he señalado en otro lugar, la configuración comunicativa del ciberespacio puede implicar que acciones cuyos efectos se producen de forma instantánea y caduca en el espacio físico, queden fijadas en el ciberespacio durante un tiempo indeterminado y sigan desplegando efectos, en este caso de afectación de la dignidad, aunque la ejecución solo fuese una y durase un instante.[26] Si tenemos en cuenta esto y a ello añadimos que, tal y como acertadamente han señalado los tribunales, el tipo básico de los delitos contra la integridad moral no exige habitualidad sino menoscabo de la dignidad, creo que es posible afirmar que la difusión de determinadas imágenes o textos degradantes en el ciberespacio adquiere un «sentido lesivo» mucho mayor que el que las mismas podían conllevar en el espacio físico. Esto no significa, en todo caso, que cualquier comunicación o difusión en Internet realizada con ánimo de burla vaya a resultar delictiva: deberá exigirse una entidad suficiente para considerar que hay lesión de la integridad moral de la víctima.

De hecho, son muchas las resoluciones que no aprecian, en casos de acoso continuado a menores en Internet, delito del art. 173 CP y reconducen la infracción a una falta de vejaciones. Así lo entienden varios tribunales en casos

20. SAP de Baleares n.º 125/2010, de 15 de marzo.
21. Como la resolución dictada recientemente por la AP de Cantabria, en la que acordaba continuar el expediente en relación con la comisión de un presunto delito del art. 173 CP, argumentando que en ese caso se encontraban «ante una situación prolongada en el tiempo, realizada presuntamente por varias menores, con un objetivo común: acosar y hostigar a otra menor» (AAP de Cantabria n.º 291/2012, de 25 mayo).
22. En este caso, la SAP de Baleares n.º 125/2010, de 15 de marzo, especifica que «los hechos se iniciaron posiblemente en el año dos mil cinco, pero continuaron los mismos con distintas facetas hasta que estallaron en mayo del 2007».
23. Acerca de la clara relación entre el *sexting* y el posterior acoso a menores, *vid*. J. R. Agustina, 2010.
24. SAP de Valencia n.º 488/2009, de 10 de septiembre.
25. STS 1218/2004, de 2 de noviembre.
26. F. Miró, *op. cit*., pág. 150.

de publicación de mensajes ofensivos,[27] perfiles falsos con comentarios vejatorios,[28] conductas calificadas como «hacerle la vida imposible» a la víctima[29] o la difusión de imágenes trucadas de una menor,[30] todos ellos llevados a cabo en la red social Tuenti.[31] Y, por supuesto, corresponde la absolución en aquellos casos, como los enjuiciados por la SAP de Córdoba n.º 59/2009, de 26 febrero, en los que lo que se difunde son imágenes no ofensivas ni denigratorias o comentarios que lo sean pero de tan escasa relevancia que no merezcan una respuesta penal.[32]

En ocasiones, por otro lado, el *cyberbullying* puede ser, como se dijo en el análisis fenomenológico, una extensión en el ciberespacio de un *bullying* tradicional que se ejerce sobre la víctima.[33] En ese caso, evidentemente, la entidad del acoso o ataque a la dignidad no debe valorarse teniendo en cuenta por separado lo ejecutado en cada uno de los ámbitos, sino la posible afectación de la dignidad moral que se puede producir por la unión de todos ellos.[34]

Por último, hay que precisar que gran parte de las formas de *bullying* continuado a menores contienen en sus dinámicas comisivas ataques suficientemente graves a otros bienes jurídicos como la libertad, la intimidad o el honor, como para ser sancionados, junto al posible atentado a la integridad moral, por medio de los diferentes tipos penales que protegen tales bienes jurídicos. La protección de tales intereses y la integridad moral tienen su nexo en art. 177 CP. Efectivamente, conforme al art. 177, si además del atentado a la integridad moral penado en el art. 173.1 se produjere lesión o daño a la vida, integridad física, salud, libertad sexual o bienes de la víctima o de un tercero, se castigarán los hechos

27. En este caso, la AP de Ourense hace responsable al menor por una falta continuada de vejaciones injustas (SAP Ourense n.º 318/2008, de 24 septiembre).
28. SAP de Segovia n.º 32/2011, de 24 mayo, que enjuicia un caso en el que se publicó el perfil falso, subiendo también hasta 56 fotos de la víctima, con comentarios que la ridiculizaban como «están llegando», en referencia a la fotografía de un platillo volante; o «no se bromea», sobre un extraterrestre; u «orgullosa de serlo», en relación a unas viñetas sobre «cómo ser un friki de provecho y no morir en el intento»; o «mis ídolos», sobre los personajes de dibujos animados de *Dragon Ball*; o «mi amor hechizado», con la fotografía del personaje de Harry Potter; «mi médico», con la imagen del personaje protagonista de *House*; o «mis ratos libres», con la imagen de la Mona Lisa; «mi inspiración», con el cuadro de la Inmaculada Concepción de Murillo; «lo mejor de lo mejor», sobre el libro de García Márquez *Cien años de soledad*; «existen», con la imagen de un espectro; «help», con la fotografía del personaje de Betty la Fea, etc.
29. SAP de Madrid n.º 400/2012, de 27 de diciembre.
30. Sentencia n.º 67/2009, de 25 febrero, del Juzgado de Instrucción de Sevilla, que sanciona como vejaciones injustas la conducta de un menor que había colocado en su perfil una fotografía manipulada en la que aparecía la víctima, compañero de su clase en el colegio, tocando un violín en el interior de una mira telescópica, compartiéndolo con todos sus contactos y provocando comentarios despectivos hacia su persona.
31. En similar sentido, también haciendo responsable a una de las acusadas por vejaciones que asimismo se sirvió de la red social Tuenti, la reciente SAP de Islas Baleares n.º 271/2012, de 26 octubre.
32. Señala el tribunal que «la mera publicación de una fotografía de grupo en la que aparece la denunciante en una actitud correcta y con una imagen que en ningún caso es ofensiva o denigratoria, no puede considerarse constitutiva de vejaciones injustas, sin perjuicio del alcance que dicha actuación pudiera tener sobre el derecho a la intimidad o a la propia imagen en la esfera civil». Añade posteriormente que «más problemática resulta, por el contrario, la tipificación de las expresiones proferidas en relación con dicha fotografía, relativas a la supuesta falta de gusto o acierto de la denunciante al arreglarse (vestirse, peinarse, maquillarse....) [...] pero no alcanzan entidad suficiente para ser consideradas infracción penal».
33. Y es que, como recuerdan M. A. Hernández e I. M. Solano (2007), hay dos tipos de *cyberbullying*: «aquel que actúa como reforzador de un *bullying* ya emprendido, y aquella forma de acoso entre iguales a través de las TIC sin antecedentes». Explican las autoras que en la primera modalidad se acude al *cyberbullying* cuando las formas tradicionales de acoso ya no son eficientes o satisfactorias para el acosador, utilizando la red para ver amplificados los efectos sobre la víctima. En esta primera modalidad, el acosador es más fácilmente identificable, puesto que ya ha habido un acoso presencial y directo. En la segunda modalidad de *cyberbullying* que formulan las autoras, sin embargo, no tiene por qué haber un motivo aparente para que se lleve a cabo el acoso, pues no hay antecedentes presenciales, es decir, el acosador no conoce previamente a la víctima. Con esta segunda modalidad parecen referirse a los casos en los que el acosador elige a la víctima al azar, de forma aleatoria a través de la Red. En este segundo caso, y como consecuencia del diferente móvil del acosador, el *cyberbullying* tendrá unas características distintas.
34. Así lo hace, acertadamente, la SAP de Granada (Sección 1.ª) n.º 462/2012, de 24 septiembre, en un caso en el que la menor acusada sometió a otra alumna de su mismo instituto de forma sistemática durante un curso escolar a una persecución y acoso caracterizado por hacerla objeto de continuas amenazas, insultos y burlas, bien de forma personal (muchas veces apoyada por un grupo de amigas que posteriormente realizaron la actividad educativa propuesta por los equipos de mediación), y finalmente a través de Tuenti publicando insultos graves a la víctima.

separadamente con la pena que les corresponda por los delitos o faltas cometidos, excepto cuando aquel ya se halle especialmente castigado por la ley.[35] Así lo hace la SAP de Málaga n.º 452/2009, de 16 de septiembre, en un supuesto en el que tres escolares agredieron en varias ocasiones a una compañera mientras una de ellas grababa la agresión en un teléfono móvil, grabación que después enviaron por Bluetooth a otros alumnos. En este caso, además de imputar en coautoría el art. 173.1 por la conducta de acoso llevada a cabo por las menores, aplican también el delito de descubrimiento y revelación de secretos, declarando que «el delito del art. 197 del Código penal en este caso viene constituido por la captación de unas imágenes que formaban parte de la intimidad de la víctima y de su derecho a la propia imagen, sin su consentimiento, y su posterior distribución entre terceras personas».[36]

Como puede advertirse, para finalizar con esta parte del trabajo, prácticamente todos los casos enjuiciados hasta el momento son de *bullying*, esto es, el agresor es también un menor. Para el caso en el que el agresor sea un adulto valdría, en todo caso, lo afirmado, con una excepción: cuando el acoso es entre menores deberá aplicarse la Ley orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad de menores, debiendo tenerse en cuenta, a la hora de la selección de las medidas que hay que aplicar, la Instrucción 10/2005, de 6 de octubre, de la Fiscalía General del Estado, que destaca que no se puede caer en la simplificación de reducir el abordaje del acoso escolar «mediante medidas puramente represivas y menos aún a su tratamiento centrado en la jurisdicción de menores, pues este enfoque simplista puede llevar a un enquistamiento del problema», y añade que «el primer nivel de lucha contra el acoso escolar debe estar liderado por los profesores del centro educativo [...]. El abordaje debe ser conjunto, y preferentemente desde los niveles básicos de intervención: padres, profesores y comunidad escolar».

3.3. La punición de actos de *online harassment* por otros preceptos del CP

Para finalizar con el análisis de la respuesta penal a las distintas formas de acoso (no sexual) a menores en el ciberespacio, conviene fijarnos en las posibilidades de sanción de ciberataques ocasionales, en el sentido de no reiterados, a la libertad, intimidad u honor entre otros intereses. Como ya se ha visto, es posible la aplicación del propio delito del art. 173 CP cuando un solo ciberataque sea de tal entidad que por sí solo pueda afectar gravemente a la integridad del menor, teniendo en cuenta, además, la especial naturaleza de Internet en cuanto a la posibilidad de que los efectos se eternicen y multipliquen en el tiempo. Pero no es la integridad moral el único bien que puede ser lesionado por alguna de las formas de ciberacoso que se han identificado. También puede haber atentados a otros bienes que, con referencia a casos en los que la jurisprudencia ha aplicado frente a concretos cibercrímenes los tipos penales que tratan de proteger los citados intereses, vamos a analizar a continuación por separado.

Empezando por el bien jurídico libertad, y dejando al margen la libertad sexual, que podría ser analizada en un futuro trabajo, sabemos que nuestro sistema penal incluye una completa protección de tal bien tanto en el momento de la

35. Estas pautas, no obstante, deben de nuevo matizarse en el caso de que sea de aplicación el Derecho Penal de Menores: si bien son plenamente aplicables en cuanto a la calificación jurídica de los hechos, a efectos de determinar la consecuencia habrá de estarse a las previsiones específicas que para determinar la medida en caso de concurso ideal se contienen en el art. 11 LORPM, de acuerdo a la interpretación contenida en el punto V.5 de la Circular 1/2000, de 18 de diciembre. En Derecho Penal de Menores no se aplica, pues, la agravación de la consecuencia jurídica prevista para el mismo supuesto en el art. 77 CP, sino que se sigue el principio de absorción.

36. Y no es esta la única resolución en la que se plantea la aplicación del art. 197 en un caso de ciberacoso entre menores, pues también el Auto de la AP de Barcelona de 27 septiembre 2006 apunta la posibilidad de su aplicación en el caso en que una menor procedió voluntariamente a la remisión de fotografías propias en las que aparece desnuda a una dirección de correo electrónico correspondiente a un amigo, quien a su vez la habría remitido a otro, hasta llegar al alcance de la «amiga» que dijo haber procedido a su colocación en una dirección de Internet. Considera la AP de Barcelona en este caso, sin embargo, que no pueden «completarse las exigencias típicas del precepto enunciado por cuanto es la propia titular que pretende vulnerada su intimidad quien dispone de ella y permite el acceso de terceros a unas fotos del carácter íntimo que sin duda tenían las remitidas por e-mail». Y concluye el tribunal que el Derecho penal «no puede desplegar sus efectos tutelares respecto de intereses o bienes jurídicos cuyo titular, y primer interesado en la protección, no ha adoptado unas mínimas cautelas autoprotectoras». Sí que se consideró, sin embargo, aplicable el delito de descubrimiento y revelación de secretos a la conducta del acusado que colgó en Tuenti una fotografía de la víctima, invitando a los compañeros y amigos a hacer comentarios sobre él, y respondiendo estos en los días siguientes con expresiones despectivas y de mofa (SAP de Murcia n.º 7/2010, de 29 enero).

toma de decisiones como en el de su ejercicio. Tal interés puede ser lesionado a través de Internet por medio de amenazas o coacciones, respectivamente, siendo mucho más frecuente la punición de las primeras cuando se realizan en el ciberespacio. Así, aunque lo más habitual son las resoluciones en las que se condena como autor del delito de amenazas a un adulto por anunciar, a través de cualquiera de los medios de comunicación que permiten Internet y la telefonía móvil, un mal a otro adulto,[37] también están comenzando a ser frecuentes conductas de acoso a menores relacionadas con el propósito de obtener imágenes de contenido sexual a través de cámara web. Tales actos pueden dar lugar a la aplicación de delitos sexuales (como el de corrupción de menores), pero también pueden ser sancionados por el delito de amenazas.[38] Y no solo en estos casos el delito de amenazas se aplicará frente a actos de este tipo en el ciberespacio: por citar una variedad de supuestos, la SAP de Tenerife n.º 541/2005, de 5 mayo, entendió aplicable el delito de amenazas al menor que realizó reiteradas llamadas a la víctima, amenazándole;

37. Por citar algunos ejemplos significativos, en la SAP de Barcelona n.º 1242/2009, de 30 de septiembre de 2009, se condena por amenazas al acusado que dirige por correo electrónico a su ex pareja expresiones tales como «si no eres para mí no serás para nadie». Similar conducta se sanciona en la SAP de Burgos de 23 de diciembre de 2002, en la que se condena al acusado por una falta continuada de amenazas por el envío reiterado y persistente de mensajes vía Internet a su excompañera sentimental, con un fondo intimidatorio que le infundía temor y desasosiego. Y también es similar la conducta sancionada en la SAP de Madrid n.º 407/2006, de 21 de noviembre de 2006, en la que se condena al acusado como autor de una falta de amenazas por enviar de forma reiterada correos electrónicos a la acusada, con la que tuvo una relación sentimental, en los que le advertía que no iría tranquila por la calle y su intención de lesionar a su novio actual. También en la SAP de Madrid n.º 1115/2007, de 28 de diciembre de 2007, en la que se condena al acusado como autor de un delito continuado de amenazas por enviar mensajes de correo electrónico a la víctima, una vez finalizada la relación con ella, en tono intimidante. En la SAP de León n.º 73/2001, de 7 de mayo de 2001, se condena al acusado como autor de una falta de amenazas porque envió tres textos por correo electrónico en los que vertía diversos insultos y amenazas contra dos mujeres. Por su parte, en la SAP de Zaragoza n.º 8/2008, de 3 de marzo de 2008, se condena por un delito de amenazas al acusado por enviar correos electrónicos, tanto a la víctima como a su actual pareja, pues se pone de manifiesto en la sentencia que «a lo largo de toda la secuencia de las mismas el acusado desplegó una conducta de contenido inequívocamente intimidatorio, que resume de manera clara y contundente, en condiciones de aptitud lo suficientemente sólidas como para hacer llegar al ánimo de los perjudicados que su vida estaba realmente en peligro, cosa que, desgraciadamente, ocurrió en el caso de Enrique». Esta sentencia posteriormente es confirmada por la STS n.º 949/2008, de 27 de noviembre de 2008. En la SAP de Barcelona n.º 370/2010, de 23 de marzo de 2010, se condena al acusado por un delito continuado de amenazas por mandar correos electrónicos a su expareja, ya que, como explica el tribunal, «efectivamente la conducta del acusado con tales expresiones intimidatorias (existe el anuncio de un mal expreso, serio, firme y que además es objetivamente capaz de causar un estado de temor en la persona contra quien se dirige) denota su intención de ocasionar inseguridad y temor a la denunciante como lo demuestra el dato que llegó a solicitar una orden de protección, y que permite llegar al convencimiento de que con las concretas expresiones proferidas por el acusado, únicamente solo un propósito le movía, cual era perturbar y atemorizar a su oponente, con independencia de que en su fuero interno existiere o no la intención de llevar a cabo lo amenazado, lo cual, es indiferente para apreciar el delito de amenazas». En similar sentido, una reciente resolución en la que se señala que «anunciar a una persona, con la que se ha mantenido una relación sentimental, más o menos duradera, que un video, grabado con su consentimiento, es verdad, de la pareja manteniendo una relación sexual, acto, en principio, perteneciente a la más estricta intimidad, va a ser difundido en Internet, a través de una plataforma pública como es YouTube, no se puede entender como una mera vejación sino que implica la amenaza de un mal que constituiría un auténtico delito de injurias y con publicidad, art. 208 y 209 del Código penal, lo que, por tanto, los llevaría a entender que nos encontramos ante una amenaza no condicional de un mal que constituiría un delito contra el honor, perfectamente sancionable al amparo del art. 169 párrafos primero y último del vigente C. Penal dado que ese acto, publicar en Internet una grabación obtenida a partir de la confianza propia de una relación sentimental y de algo tan íntimo como un encuentro sexual, no puede calificarse sino como un acto destinado a lesionar la dignidad de otra persona y a menoscabar su fama o su propia estimación [...]» (SAP de Las Palmas n.º 449/2008, de 9 de diciembre de 2008).

38 Así, la SAP de Vizcaya n.º 759/2008, de 18 de noviembre de 2008, condenó al acusado, además de por otros delitos relativos a la corrupción de menores, por un delito de amenazas. Explica la sentencia que el acusado obligó a una chica de 15 años a que se realizara tocamientos y masturbaciones ante su cámara web y detalla la sentencia que «en la primera ocasión, el acusado la amenazó con difundir entre sus amigos los correos personales de los que se había apoderado y en la segunda, la amenazó con difundir entre sus amigos las grabaciones que decía haber obtenido de ella e, incluso, le dijo que las colgaría en "Internet", e intentó bajo presión, también, conseguir un encuentro con la menor con el fin de mantener con ella relaciones sexuales. Resulta pues acreditado que el acusado en la medida que con tales requerimientos y amenazas logró vencer la voluntad de la menor y dar satisfacción a sus deseos sexuales inició a la menor en la ejecución de actos libidinosos encaminados a su corrupción, no se trataba de ningún juego como ya se ha expresado, y sin duda esta conducta ha causado en Aurelia un perjuicio en su libertad e indemnidad sexual pues, según ella misma declara y ratifica su madre, siguió tratamiento psicológico aunque fuera por tiempo breve».

la SAP de Castellón n.º 115/2011, de 12 abril, que también hace responsable por el delito de amenazas al menor que pretendió amedrentar a otro mediante reiterados correos electrónicos; o la SAP de La Rioja n.º 8/2006, de 17 enero, que consideró responsable de una falta del art. 620.2 al menor que envió varios mensajes de teléfono móvil al primero diciéndole «subnormal; deja a Lucía o te parto la cara», así como «que le iba a dar un tortazo» y «que le iba a dar dos hostias bien dadas».[39]

Este tipo de conductas, sin embargo, no siempre son situadas por nuestros tribunales en el ámbito punitivo de las amenazas, siendo calificadas en algunos casos como coacciones.[40] Lo cierto es que algunos de estos comportamientos no afectarán únicamente a la libertad en el proceso de formación de la voluntad, sino a la misma libertad de obrar, y la exagerada tendencia de algunos tribunales a aceptar la espiritualización del elemento «violencia» en las coacciones puede llevar a la calificación como coacciones de hechos más cercanos a la violación de la libertad decisoria y no ejecutoria. En este sentido resulta interesante la SAP de Barcelona n.º 381/2009, de 14 de abril de 2009, que condenó como autor de un delito de difusión de pornografía infantil utilizando menores de trece años y de un delito de coacciones, a un sujeto que, aprovechando el anonimato de Internet, se hizo pasar por un adolescente para conseguir que una menor de 14 años le mandara fotos de ella desnuda, amenazándola posteriormente con difundirlas si no le mandaba más fotos suyas y de su hermana de 9 años.[41] Tal resolución fue recurrida ante el TS, que, por medio de la STS n.º 1107/2009, de 12 de noviembre de 2009, anuló parcialmente la sentencia en el sentido de sustituir la condena de coacciones por amenazas,[42] argumentando que los elementos constitutivos del delito de coacciones no concurren en los hechos enjuiciados, pero sí los del delito de amenazas condicionales. Señala el tribunal que aunque el bien jurídico protegido en ambos delitos es el mismo, la coacción exige violencia, que no puede ser ampliada expandiendo el ámbito del delito, y también una mayor inmediación entre el coaccionante y el coaccionado en cuanto a la actividad del primero de torcer la voluntad del segundo; todo lo cual no concurre en un caso en el que la víctima se negó a enviar fotos de ella desnuda, ante lo cual «el autor no ejerce ninguna fuerza física ni psíquica, sino que pone en marcha una conducta típica del delito de amenazas, contemplada en el artículo 169 del Código penal; es decir, amenaza a la menor con causarle un mal que en este caso concreto afecta a su integridad moral, a

39. Y en este último sentido, aplicando también una falta de amenazas, se pronuncia la SAP de Cádiz n.º 118/2012, de 17 abril, en la que un menor amenazó a otro a través de Tuenti. Aunque se pueden encontrar también escasas absoluciones, como la SAP de Soria n.º 83/2012 de 15 noviembre.

40. Así lo hace la SAP de Granada n.º 283/2009, de 25 de mayo de 2009, en la que se condena al acusado, además de por otros delitos relativos a la corrupción de menores, por seis faltas de coacciones y no por delito de amenazas. Consta en los hechos probados de la sentencia que el acusado mantenía contacto con las víctimas a través de un chat y realizaba conductas dirigidas a conseguir que los menores le enseñaran sus genitales a través de su cámara web. De nuevo, y pese a la calificación de los hechos como coacciones, los hechos relatados en la resolución parecen cuadrar más bien en el ámbito de las amenazas: «Uno de los menores dijo que le amenazó diciéndole que era un policía y que si no mandaría sus fotos por Internet, luego le dijo que era profesor de informática y por su bien que lo aceptara en el Messenger. Otra víctima dijo que no recordaba si le había amenazado con mandarle un virus, pero si se acuerda que le dijo que le iba a mandar a su padre las facturas de los códigos. Otra víctima dijo que le amenazó con mandarle un virus o algo así, pero lo veía una tontería y no llegó a sentir miedo con las amenazas. Otra víctima dijo que un par de veces le amenazó con que si decía algo lo buscarían en Mallorca, y que le podía infectar el ordenador con un virus. Otra víctima manifestó que cuando pasaban de él, los amenazaba, diciendo que les podía hacer daño. Y otra víctima dijo que le amenazó con ir a buscarlo a su casa y mandarle un virus.» Curiosamente, la propia resolución reconoce que no se daba en el caso enjuiciado «una violencia psíquica de tal intensidad y grado de malicia que constriñera gravemente la legítima voluntad y libertad de los menores, ni existía una idoneidad de medios para su imposición; en tanto que lo desconectaban cuando les parecía, y en otras ocasiones no le hacían mucho caso, y trataban de engañarlo para conseguir sus recargas a los móviles o códigos de juegos».

41. Explica la sentencia que «en el presente caso, atendidas las circunstancias personales de la víctima, una menor de 14 años, el modo de comisión de los hechos como fue el aprovechamiento por el acusado del anonimato que permite Internet, simulando ser persona adolescente para lograr sus objetivos pues es evidente que Penélope, de tener conciencia de la edad del acusado, nunca le habría permitido tener acceso a su persona a través de Internet, así como lo que constituyó el objeto y finalidad de la exigencia y la conminación del mal, revelan en el acusado una malicia que obliga a calificar las coacciones como graves y, por ende, constitutivas del delito del artículo 172».

42. Lo cual, como el propio tribunal recuerda, no es problemático, dado que a partir de la sentencia de 23 de noviembre de 1989 y 5 de julio de 1990, «hasta la más reciente de 19 de junio de 2009, siempre se ha considerado que las amenazas y las coacciones son delitos homologables, por lo que no vulnera el principio acusatorio el cambio de calificación jurídica».

su intimidad y honor, e incluso a su autodeterminación en su comportamiento sexual».[43]

Cuestión distinta, lógicamente, sería si la comunicación del sujeto activo con el sujeto pasivo sirviera para impedir al sujeto hacer lo que la ley le permite. Esto es lo que se ha interpretado por parte de varias audiencias provinciales en casos de envío de SMS[44] o de correos electrónicos, que, independientemente de su capacidad para amenazar, suponen ya una intromisión en la libertad ejecutiva del sujeto de mantener ese tipo de comunicación con una persona con la que no quieren hacerlo.[45] Lo complejo en estos casos, sin embargo, es la extensión del concepto de violencia que se produce cuando se entiende que la intimidación producida a través de correos electrónicos y de la amenaza de publicar contenidos íntimos en Internet es equiparable a la fuerza. A mi parecer, aciertan las resoluciones que suelen calificar estas conductas como coacciones leves constitutivas de falta,[46] pues solo extraordinariamente, cuando la intimidación ejercida a través del ciberespacio sea tan grave como para ser considerada una vis compulsiva impeditiva, podrá entenderse la misma equivalente a la fuerza exigida para la violencia en las coacciones. En el resto de los casos estaremos, más bien, ante amenazas condicionales que, en muchos casos, también serán agravadas si se acaba cumpliendo la condición exigida.

Menos complicada parece la apreciación de delitos contra el honor cometidos contra menores a través del ciberespacio, como demuestra el amplísimo catálogo de sentencias de audiencias provinciales en las que se condena como autores de delitos o faltas de injurias a sujetos que realizan tales conductas a través de Internet. Así, por medio de la publicación de fotos obscenas o denigratorias en páginas web[47]

43. Añade la sentencia que «el componente de la amenaza era claro y estaba claramente expuesto. La menor pudo perfectamente negarse sopesando las consecuencias o bien, como era de esperar, ceder ante el amenazante para evitar un mal concreto y específico y no genérico como en la coacción. Si se negaba, colgaría en la red las fotos de las que ya disponía y las divulgaría lesionando con ello su honor e intimidad, su integridad moral y su capacidad de autodeterminarse sexualmente. El mismo hecho probado no sitúa ante situación de ponderación de males al añadir que por encima de las conminaciones, la menor, más adelante, decidió negarse a ceder al chantaje y cortó toda relación con el acusado [...]».
44. Es lo que ocurre en el supuesto enjuiciado por la SAP de Zaragoza n.º 374/2003, de 20 de noviembre de 2003, que califica como coacciones la conducta de un sujeto que enviaba través de Internet mensajes a los teléfonos móviles de su excompañera sentimental y unas amigas, con frases de contenido sexual insultante, con la intención de conseguir el aislamiento del grupo; y lo consiguió, pues el grupo se desintegró, al menos en lo que respecta a esta última, «utilizando una intimidación en modo alguno permitida y que ha de considerarse como grave».
45. Son paradigmáticas en este sentido las tres resoluciones siguientes: la SAP de Madrid n.º 1097/2009, de 30 de septiembre de 2009, que condena al acusado por el envío reiterado de correos electrónicos a su ex pareja, «pretendiendo determinar cómo ha de transcurrir su vida, estableciéndole reglas de conducta, cuestionando de forma constante su actuación como madre, utilizando, también continua y reiteradamente a su hijo como instrumento de presión, de chantaje emocional, para obligarla a admitir sus constantes intrusiones, contra su voluntad, expresa y reiterada [...]»; la SAP de Pontevedra n.º 15/2009, de 29 de enero de 2009, que condena al acusado por un delito de coacciones hacia su expareja alegando que quedaba acreditado que el acusado le enviaba, de manera reiterada y constante, correos electrónicos, «produciéndole inquietud y desasosiego»; y también la SAP de Barcelona n.º 522/2009, de 14 de abril de 2009, que condena por un delito continuado de coacciones al acusado, por la presión que ejerció hacia la víctima mediante el envío de correos electrónicos, ya que aquella no quería mantener con el mismo ningún contacto, y en contra de su voluntad el acusado persistió «a través de herramientas como el correo electrónico, que eran de uso imprescindible para el trabajo, como es el caso de la perjudicada, que recibía esos correos del acusado en su dirección de la universidad». Más discutible resulta en este caso la calificación como coacciones (concretamente coacciones en el ámbito familiar) llevada a cabo por la SAP de Madrid n.º 718/2010, de 30 de abril de 2010, en la que se enjuicia el comportamiento de un sujeto que tras convivir con la víctima durante un tiempo, le remitió diversos mensajes de correo electrónico en los que le hacía saber su intención de reanudar la relación sentimental, sin obtener un resultado positivo en sus intentos, por lo que las comunicaciones se tornaron insistentes, pese a conocer la oposición de la víctima a recibir esos mensajes. Según relata la sentencia, «a consecuencia de ello, el acusado le remitió al menos 15 mensajes de correo electrónico, a algunos de los cuales adjuntó fotografías, incluyendo en algunos casos unas de ambos desnudos y manteniendo relaciones sexuales; mientras que en uno le remitía un enlace a la página web www.Morbocornudos.com, página en la que aparecen diversas mujeres manteniendo relaciones sexuales bajo la rúbrica de tratarse de exnovias y exmujeres de diferentes hombres, envío que acompañó del texto "imagínate en esta web". Como consecuencia de esta situación la víctima sufrió un trastorno adaptativo con síndrome depresivo por el que precisó asistencia y terapia psicológica». Además de que resulta complicado describir el comportamiento como realizado «con violencia», la libertad afectada aquí es más la decisoria que la de obrar.
46. Así, por ejemplo, la SAP de Vizcaya n.º 615/2004, de 1 de septiembre de 2004, que condena al acusado como autor de una falta de coacciones, por intentar, a través del envío de correos electrónicos, que la víctima se relacione con él y contra la voluntad de la víctima.

o de su remisión por e-mail a personas determinadas,[48] del envío de correo electrónico a sujetos concretos[49] en los que se realizan declaraciones atentatorias del honor y la dignidad de las personas,[50] de la publicación en blogs de expresiones insultantes dirigidas a una persona en particular,[51] del envío por Messenger de mensajes con semejante contenido,[52] de la publicación en foros de opinión de expresiones insultantes,[53] o incluso mediante conductas atentatorias del honor más elaboradas como la consistente en insertar en varias direcciones de Internet diversos anuncios en los que se incitaba a llamar al teléfono de la perjudicada con la finalidad de tener una conversación de tipo sexual,[54] el ciberespacio es fuente inagotable de atentados contra el honor de las personas que merecen una respuesta penal proporcionada por medio del delito de injurias del artículo 208 CP, y de la falta del artículo 620.2 CP, según la gravedad; e incluso del delito de calumnias del artículo 205 cuando lo que se difunda a través de Internet sea la comisión de un delito.[55] Hay que tener en cuenta, además, que el artículo 209 agrava la pena de las injurias (y el artículo 206, la de las calumnias) cuando el hecho se realizase con publicidad. Excepto en los casos en los que se transmita la injuria por medio de correo electrónico, SMS o cualquiera de las formas de mensaje directo a un destinatario que permiten las TIC, este agravante se aplicará en todos los demás supuestos tales como difusión de mensajes en páginas web, foros, redes sociales, etc., cuando el mensaje se ponga a disposición de un número indeterminado de sujetos.[56]

Conclusiones

Podría afirmarse, por tanto, que pese a las problemáticas aparentes que plantea la ausencia de tipificación expresa

47. La SAP de Cádiz n.º 75/2005, de 22 de abril de 2005, condena al acusado como autor de una falta de injurias por colgar en una página de Internet unas fotos obscenas de la denunciante.
48. De este tipo son los hechos enjuiciados en la SAP de Palencia n.º 32/2006, de 28 de junio de 2006, que condena al acusado como autor de un delito de injurias graves con publicidad, por enviar a dos amigos fotos de su exnovia desnuda, que, además, cuelga posteriormente en diversas páginas de Internet, no existiendo posibilidad de quitarlas. Detalla la sentencia que «sería suficiente con el hecho de que se hubiesen remitido las fotos por medio de un fichero a los llamados Alexander y Aurelio para entender que se hubiese cometido el delito de injurias, pero a mayor abundamiento se ha dado también por acreditada la inmisión en páginas de Internet de un programa conteniendo las mismas fotografías, y tal acción es encuadrable en el tipo penal en cuestión».
49. La SAP de Castellón n.º 10/2003, de 18 de enero de 2003, condena al acusado como autor de un delito continuado de injurias graves con publicidad, por realizar una campaña de descrédito contra un abogado en base al desacuerdo con la intervención profesional de este en su proceso de separación, enviando varios correos electrónicos al buzón del Colegio de Abogados, sin mayor publicidad que la de los empleados del colegio que abrían el correo, faltando en sus comentarios al letrado.
50. Es el caso de la SAP de Murcia n.º 9/2003, de 29 de enero de 2003, que condena al acusado por proferir injurias a través de mensajes en Internet «empleando reiteradamente los términos "puta", "gorda" y "zorra" en referencia a esta última.- Asimismo, en el mensaje remitido el día seis de marzo le decía: "... y cuidado con las palizas", en referencia a una agresión que la Sra. Clara había sufrido anteriormente». También en la misma audiencia provincial se condena, en la SAP de Murcia n.º 194/2009, de 20 de julio de 2009, a un sujeto como autor de una falta de injurias leves por presentar, vía Internet, una reclamación contra la directora de la biblioteca municipal, refiriéndose tanto a ella como a otra trabajadora de esa biblioteca con expresiones insultantes.
51. En la SAP de Lleida n.º 184/2010, de 25 de mayo de 2010, se condena al acusado como autor de una falta de injurias por poner en un blog de Internet expresiones como "alcohólico" dirigidas al alcalde.
52. En el caso de la SAP de Lleida n.º 159/2010, de 7 de mayo de 2010, que condena al acusado como autor de una falta de injurias por enviar expresiones a la víctima por el Messenger como "puto diablo colombiano, basura operada de quirófano, muérete ramera, prostituta colombiana y escoria".
53. Así son los hechos enjuiciados en la SAP de Murcia n.º 134/2009, de 21 de octubre de 2009, que condena a la acusada por una falta de injurias.
54. Suceso enjuiciado por la SAP de Navarra n.º 124/2004, de 29 de junio de 2004, que condenó por el mismo a la acusada como autora de un delito de injurias graves con publicidad.
55. Tal y como sucede, por ejemplo, en la SAP de Asturias n.º 174/2004, de 20 de mayo de 2004, que condena al acusado por dos delitos de calumnias por la publicación en un foro de una página web de Internet de una información en la que se imputaba a las querellantes la apropiación de fondos pertenecientes a una sociedad, que pudiera ser constitutiva de un delito de malversación de caudales o fraude de subvenciones; la SAP de Sevilla n.º 152/2000, de 6 de marzo de 2000, que condena a un periodista que publica en un periódico de Internet un anónimo que contiene una imputación falsa de hechos que pueden constituir delitos de prevaricación, cohecho y colaboración con banda armada, añadiendo consideraciones propias para conferir mayor verosimilitud a los hechos; y en similar sentido la SAP de Zaragoza n.º 197/2008, de 1 de abril de 2008.
56. E. Orts, M. Roig, 2001.

de los delitos de *cyberbullying* o de *cyberharassment,* el Código penal, a través de los distintos tipos penales que regulan intereses esenciales de los menores tales como la dignidad, la intimidad, el honor o la libertad, responde adecuadamente a los principales ataques a los mismos cometidos a través de Internet. Lo hace frente al *cyberbullying*, cuando el acoso al menor por parte de otro menor se concrete en una continuidad de acciones que afecten a su integridad moral; y también cuando, pese a no existir actos repetidos de ciberacoso, la entidad del ataque sea tal que se pueda considerar lesionado tal bien jurídico. También se responde adecuadamente a los más graves actos que conforman esa macrocategoría fenomenológica que es el *online harassment*. Por medio, muy especialmente, de los delitos de amenazas, en ocasiones también por medio de las coacciones cuando sea posible interpretar que hay una vis compulsiva que impide realizar lo no prohibido, y por medio de los delitos de injurias y calumnias, así como por otros delitos como los de descubrimiento y revelación de secretos.

Aun así, seguirá existiendo la tentación, esencialmente por el potencial comunicativo que conlleva, de una tipificación expresa de estos delitos. En el momento en que surja el último dramático caso de suicidio relacionado con algún tipo de ciberacoso, se discutirá la necesidad de una regulación expresa de tales conductas. Con el régimen actual, sin embargo, no solo se responde a todas las conductas que deben merecer un reproche penal, sino que además los jueces disponen de una variedad de tipos penales, relacionados con distintos intereses jurídicos, que permite una respuesta proporcionada y adecuada a la lesión que cada una de las conductas conlleve sobre los bienes jurídicos. La creación de un tipo penal de ciberacoso o de *cyberbullying* probablemente no mejoraría la respuesta penal a este tipo de conductas.

Bibliografía

AGUSTINA, J. R. (2010). «¿Menores infractores o víctimas de pornografía infantil? Respuestas legales e hipótesis criminológicas ante el *Sexting*». *Revista Electrónica de Ciencia Penal y Criminología*, n.º 12-11, págs. 11:6 y 11:34.
<http://criminet.ugr.es/recpc>

BASU, S.; JONES, R. (2007). «Regulating cyberstalking». *Journal of Information Law & Technology*. Vol. 22, pág. 13.

BOCIJ, P. (2003). «Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet». *First Monday Peer-Reviewed Journal on the Internet*. Vol. 8, n.º 10.
DOI: http://dx.doi.org/10.5210/fm.v8i10.1086

BOCIJ, P.; MCFARLANE, L. (2002). «Online harassment: Towards a definition of cyberstalking». *Prison Service Journal*. Vol. 139, págs. 31-38.

CALMAESTRA, J. (2011). *Cyberbullying: prevalencia y características de un nuevo tipo de bullying indirecto* [tesis doctoral]. Córdoba: Servicio de Publicaciones de la Universidad de Córdoba, pág. 48 y ss.

FARRINGTON, D.P. (1993). «Understanding and Preventing Bullying». *Crime and Justice*. Vol. 17, pág. 384.
DOI: http://dx.doi.org/10.1086/449217

HEINEMANN, P. P. (1969). «Apartheid». *Liberal Debat*, n.º 2, págs. 3-14.

HENSON, B. (2010). «Cyberstalking». En: B. FISHER, S. LAB (eds.). *Encyclopedia of victimology and crime prevention*, pág. 253.

HERNÁNDEZ, M. A.; SOLANO, I. M. (2007). «Ciberbullying, un problema de acoso escolar». *Revista Iberoamericana de Educación a Distancia*. Vol. 10, págs. 17-36.

MARCO, J. J. (2010). «Menores, ciberacoso y derechos de la personalidad». En: J. GARCÍA (coord.). *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch.

MIRÓ, F. (2012). *El cibercrimen. Fenomenología criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons, pág. 91.
DOI: http://dx.doi.org/10.1049/el.2012.2349

MIRÓ, F. (2011). «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen». *Revista Electrónica de Ciencia Penal y Criminología*, n.º 13-07.

OLWEUS, D. (1998). *Conductas de acoso y amenaza entre escolares*. Madrid: Morata, pág. 25.

OLWEUS, D. (1994). «Bullying at school. Long-term outcomes for the victims and an effective school-based intervention program». En: L. R. HUESMANN. *Aggressive Behavior: Current Perspectives*. Nueva York: Plenum Press, págs. 97-130.
DOI: http://dx.doi.org/10.1007/978-1-4757-9116-7_5

ORTS, E.; ROIG, M. (2001). *Delitos informáticos y delitos comunes cometidos a través de la informática*. Valencia: Tirant lo Blanch, pág. 146.

ORTEGA, R.; DEL REY, R.; MORA-MERCHÁN, J. (2001). «Violencia entre escolares. Conceptos y etiquetas verbales que definen el fenómeno del maltrato entre iguales». *Revista Interuniversitaria de Formación del Profesorado*, n.º 41, pág. 100.

PARDO, J. (2010). «Ciberacoso: cyberbullyng, grooming, redes sociales y otros peligros». En: J. GARCÍA (coord.). *Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*. Valencia: Tirant lo Blanch, pág. 56.

PATCHIN, J. W.; HINDUJA, S. (2006). «Bullies Move Beyond the Schoolyard: A Preliminary Look at Cyberbullying». *Youth Violence and Juvenile Justice*. Vol. 4, 2, pág. 152.
DOI: http://dx.doi.org/10.1177/1541204006286288

PATHÉ, M.; MULLEN, P. E. (1997). «The impact of stalkers on their victims». *The British Journal of Psychiatry*, n.º 170, pág. 12.
DOI: http://10.1192/bjp.170.1.12

SMITH, A. (2009). *Protection of Children Online: Federal and State Lawes Addressing Cyberstalking, Cyberharassment and Cyberbuylling*. Congressional Research Service Reports for the People, pág. 4.
DOI: http://10.1177/1461444809341263

SMITH, P. K.; MAHDAVI, J.; CARVALHO, M.; FISHER, S.; RUSSELL, S.; Y TIPPETT, N. (2008). «Cyberbullying: Its nature and impact in secondary school pupils». *Journal of Child Psychology and Psychiatry*. Vol. 49, n.º 4, pág. 376.
DOI: http://dx.doi.org/10.1111/j.1469-7610.2007.01846.x

VANDEBOSCH, H.; VAN CLEEMPUT, K. (2009). «Cyberbullying among youngsters: profiles of bullies and victims». *New Media & Society*. Vol. 11, n.º 8, pág. 1.351.
DOI: http://10.1177/1461444809341263

Cita recomendada

MIRÓ, Fernando (2013). «Derecho penal, *cyberbullying* y otras formas de acoso (no sexual) en el ciberespacio». 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. 61-75. UOC. [Fecha de consulta: dd/mm/aa]
<http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-miro/n16-miro-es>
DOI: http://10.7238/idp.v0i16.1838

Sobre el autor

Fernando Miró Llinares
fmiro@umh.es
http://fernandomirollinares.es/

Facultad de Ciencias Sociales y Jurídicas
Universidad Miguel Hernández de Elche
Avda. de la Universidad, s/n
03202 Elche

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

Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales[1*]

Lorenzo Picotti
Catedrático de Derecho penal y de Derecho penal de la informática. Università degli Studi di Verona (Italia)

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

Resumen
Este análisis de los comportamientos ilícitos en el uso y el abuso de las redes sociales se centra, en primer lugar, en los delitos que estas conductas pueden configurar (epígrafes 3 a 6) –algunos de ellos de reciente introducción, como el de *child grooming*– en que los usuarios de las redes pueden ser tanto autores como víctimas de las violaciones de los derechos fundamentales a los que tales conductas afectan (epígrafe 2). En segundo lugar, se trata la cuestión de la posible responsabilidad penal de los gestores de las redes sociales –que se pueden reconducir a la categoría general de los *Internet service providers*- que están asumiendo un papel cada vez más incisivo y protagonista en la evolución del sistema y, por tanto, también en las estrategias de prevención y control de las actividades ilícitas en la red (epígrafe 7). Los principales aspectos críticos surgidos de la presente investigación sugieren algunas indicaciones iniciales para adecuar el Derecho penal que regula esta materia a las necesidades que presenta

1. Este artículo aparecerá publicado en dos números consecutivos de la revista. En este número se tratarán los epígrafes 1 a 3, correspondientes a la introducción en primer lugar, a la consideración de los usuarios de las redes sociales como víctimas y como autores de los delitos en segundo, y por último al primer grupo de delitos analizado: el correspondiente a los delitos contra la *privacy* y contra la inviolabilidad informática. El resto de los grupos de delitos analizados aparecerán en el próximo número, así como la cuestión de la responsabilidad penal de los gestores de las redes sociales y las conclusiones del trabajo.

* Traducción de María José Pifarré de Moner, profesora agregada de la Universitat Oberta de Catalunya.

Palabras clave
delitos informáticos, redes sociales, responsabilidad penal de gestores de redes sociales, *child grooming*, delitos contra la *privacy*, delitos contra los derechos de autor

Tema
delitos en redes sociales

Fundamental Rights in the Use and Abuse of the Social Networks in Italy: Criminal Aspects

Abstract
This analysis of criminal behaviour in the use and abuse of social networks focuses, firstly, on the crimes that this behaviour can lead to (epigraphs 3 to 6) – some of which have been introduced recently, such as child grooming – where users of these networks can be both the offender or victim in the violation of the fundamental rights affected by such behaviour (epigraph 2). Secondly, it looks at the question of the possible criminal responsibility of social network managers – who are taking on an increasingly incisive role and becoming more important agents in the system's evolution, and, thus, also in the strategies for preventing and controlling criminal activities on the web (epigraph 7). The main critical aspects arising from this research highlight initial indications for how to adapt the criminal law regulating this area to the current needs.

Keywords
computer crime, social networks, criminal responsibility of social network managers, child grooming, crimes against privacy, crimes against copyright

Subject
Crime on social networks

1. Introducción: Expansión y riesgos de las redes sociales

La tumultuosa difusión de las redes sociales constituye uno de los efectos más recientes y llamativos del impacto de Internet sobre las relaciones interpersonales entre sujetos de todas las edades, profesiones y orígenes sociales –aunque de manera especial entre los jóvenes–, además de las relaciones entre el ciudadano y los entes de cualquier tipo. Ello demuestra la gran relevancia, no solo de la evolución tecnológica en sí misma, sino sobre todo de la penetración masiva que esta está teniendo en la sociedad contemporánea, en la que está determinando cambios muy importantes en los modos de comunicación y difusión de las ideas y de las informaciones, en los tiempos y contenidos del diálogo social o incluso en las costumbres, condicionando y modelando la evolución de comportamientos colectivos e individuales incluso en el mundo «real». Esto ha quedado reflejado, de manera emblemática, en los encuentros, debates, manifestaciones y movimientos políticos que se organizan en poquísimo tiempo a través de la red, o bien en ciertos hechos sorprendentes ocurridos recientemente, o

incluso en los trágicos finales a los que han llegado algunas personas a consecuencia de lo sucedido o preanunciado en una red social.[2]

Junto a estos nuevos problemas de naturaleza social, cultural, psicológica y hasta política que el fenómeno presenta, no son menos importantes aquellos de naturaleza jurídica que inciden en la esfera de los derechos fundamentales. En estas páginas nos ceñiremos a las cuestiones que presenten relevancia penal. Antes de abordarlas, sin embargo, se hace necesario subrayar que, en el aspecto fenomenológico, el fuerte impacto innovador de las redes sociales no reside solo en la gran facilidad y velocidad de circulación y difusión de los datos, «materiales» y contenidos de todo tipo a través de la red, sino sobre todo en la tendencia a «compartirlas» en círculos que se extienden a otros usuarios y sujetos, potencialmente de cualquier parte del mundo. Los nuevos instrumentos tecnológicos permiten, efectivamente, el uso contemporáneo de una enorme cantidad de informaciones, imágenes, obras artísticas, musicales, cinematográficas o literarias, e incluso de vídeos *amateur*, fotografías, grabaciones vocales, expresiones de opinión, escritos, contribuciones propias o ajenas, «diarios» de vida personal o social, recortes o partes de periódicos o revistas o, en fin, cualquier otra cosa que se considere interesante mostrar o permitir que otros tengan a su disposición.

El usuario de las redes sociales carga (*upload*) y descarga (*download*) todo este complejo conjunto de datos de manera directa y autónoma en su cuenta, y la mayoría de las veces los pone a disposición de familiares, «amigos», compañeros o sujetos diversos con los que establece o mantiene contacto a distintos niveles. Esos datos pueden permanecer en el tiempo y se pueden extender rápidamente en cascada a otros círculos de personas y sujetos, entre los que se incluyen entes, grupos o asociaciones, hasta implicar sin distinciones al público general que, a nivel global, pueda conectarse y acceder a ellos, generalmente registrándose previamente.

Por tanto, las redes sociales, y de manera más amplia también la llamada *web 2.0* en la que estas se encuentran, se caracterizan por una gran *autonomía* de gestión individual y, al mismo tiempo, por una importante posibilidad de *interacción* entre los distintos sujetos que participan en ellas, por lo que se manifiesta así de la manera más intensa posible la dimensión generalizada y «globalizadora» del *ciberespacio*, al que se deslocaliza de manera progresiva una parte cada vez más consistente de la vida cotidiana de las personas y de los entes públicos y privados, y que llega a abarcar los ámbitos más dispares: del ocio al tiempo libre, de la cultura a la investigación, de la economía a la política, de la vida privada a las relaciones personales, sociales y públicas.

En este multiforme y articulado ambiente se manifiestan nuevas ocasiones específicas y modos inéditos de comportamientos que lesionan derechos e intereses ajenos, entre los que se incluyen los derechos fundamentales que iremos mencionando y que asumen diferente relevancia penal. Ello hasta el punto de que desde hace un tiempo la cuestión es motivo de estudio y reflexión desde muy diversos frentes, que incluyen tanto la doctrina penal[3] como, de manera más reciente, intervenciones muy autorizadas de la jurisprudencia europea[4] y de la legislación penal tanto

2. Se hace referencia, a mero título de ejemplo, a movimientos políticos de gran difusión que han abarcado toda Italia, que se han organizado, recogen adhesiones, promueven iniciativas, deliberan participaciones en campañas electorales y deciden listas de candidatos y otras cuestiones a través de la red. Es ya frecuente el uso de *Twitter* o *Facebook* para convocar manifestaciones y encuentros de todo tipo, tanto públicos como privados. Por desgracia, la crónica de sucesos contiene varios casos de suicidios o autolesiones inducidos sobre víctimas de *cyberbullying*, o bien cometidos con preanuncio o ejecutados *on-line*, que ocurren o pueden ocurrir tanto dentro como fuera del ámbito de una red social.
3. Entre las contribuciones más recientes, aunque con una atención especialmente dirigida a las infracciones contra la propiedad intelectual, véanse Flor (2012) y Nieto Martín (2010). En la literatura norteamericana, la atención se centra sobre todo en los aspectos procesales surgidos acerca de la posibilidad de utilización de las redes sociales para descubrir y buscar pruebas de delitos, incluidos los casos en que los agentes simulan identidades ficticias. Para las referencias esenciales, véase «Use of social network websites in investigations» en /Wikipedia.org/Wiki/. Sobre este tema, en la doctrina alemana, véase la reciente contribución de Hoffman (2012), que se enfrenta a los límites de las garantías, incluidas las de rango constitucional, sosteniendo que no es posible la apreciación de violación alguna de los derechos que conciernen a la intimidad de sujetos que hayan confiado voluntariamente sus datos personales a la red sin verificar la identidad de los sujetos a quienes los hacen accesibles, especialmente en la página 140, con citas ulteriores.
4. Hay que señalar, sobre todo, la importante sentencia del Tribunal de Justicia de la Unión Europea de 16 de febrero de 2012 (causa C-360), sobre la cual véase más abajo el epígrafe 7.

italiana[5] como de la Unión Europea[6], e incluso instrumentos internacionales.[7]

A pesar de ello, en Italia aún no se ha llevado a cabo un estudio sistemático de estos comportamientos ilícitos desde el punto de vista penal y de su carga de ofensa contra los derechos fundamentales. Por tanto, en este trabajo se pretende ofrecer una primera aproximación sistemática de carácter general que considere, en primer lugar, los delitos que pueden configurar las conductas de uso y abuso de las redes sociales, con especial atención a que los usuarios pueden ser tanto autores como víctimas de las violaciones de los derechos fundamentales en juego (epígrafes 2 a 6); en segundo lugar se tocará la cuestión de la posible responsabilidad penal de los gestores de las redes sociales, que pueden ser reconducidos a la categoría general de *Internet service providers* (ISP) o, según la terminología comunitaria, de los «proveedores» de «servicios de la sociedad de la información»,[8] que están asumiendo un papel cada vez más incisivo en la evolución del sistema y, en consecuencia, también en las estrategias de prevención y control de las actividades ilícitas a través de la red, incluida la salvaguardia de los derechos fundamentales en el ciberespacio (epígrafe 7).

Sin pretender llegar a conclusiones sobre la materia, dado el carácter completamente preliminar de esta investigación, se intentará ofrecer alguna indicación final acerca de los principales aspectos críticos que vayan emergiendo y acerca de las correspondientes exigencias de adecuación y desarrollo de la respuesta del Derecho penal en este campo (epígrafe 8).

2. Los delitos en las redes sociales: los usuarios como autores y como víctimas

Tal como la doctrina y la jurisprudencia de todo ordenamiento jurídico han tenido ocasión de subrayar desde hace tiempo, la difusión de la informática –especialmente tras la puesta a disposición del público del acceso y la utilización de Internet, que se puede situar a mediados de los años noventa del pasado siglo–[9] ha determinado la aparición y el desarrollo creciente de «nuevos» delitos, que se manifiestan, sea como delitos informáticos «en sentido estricto» (es decir, que ya a nivel normativo, tras su incriminación específica por parte del legislador, requieren necesariamente entre sus elementos constitutivos la utilización de las tecnologías y productos informáticos, o la producción de efectos típicos sobre ellos; piénsese en los fraudes informáticos, las falsificaciones y los daños informáticos, en los accesos no consentidos a los sistemas informáticos, etc.), sea como delitos informáticos «en sentido amplio», y en especial los delitos «cibernéticos».[10]

Estos últimos, a pesar de que pueden ser concebidos o tipificados prescindiendo de referencias a la tecnología informática y a Internet, encuentran en estos instrumentos y en general en el ciberespacio una posibilidad y modalidad peculiar de realización que generalmente los hace más temibles o dañinos, hasta el punto de que pasan a requerir una respuesta penal más específica y a menudo más severa (piénsese en la pornografía infantil o en las infracciones de los derechos de autor, pero también en las injurias o calumnias, o en otros delitos de «manifestación del pensamiento» on-line: *infra* epígrafes 4, 5 y 6), y al mis-

5. Véase especialmente el nuevo delito de *child grooming* (ciberacoso de menores) introducido mediante la Ley de 1 de octubre de 2012, número 172, de ratificación y transposición del llamado Convenio de Lanzarote (véase la nota 6), de la que se hablará ampliamente en el epígrafe 4.
6. Tómense en consideración especialmente la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los niños y la pornografía infantil, por la que se deroga la Decisión Marco 2004/68/JAI del Consejo, cuyo art. 6 prevé precisamente la obligación de introducir el delito indicado en la nota anterior.
7. Véase el Convenio del Consejo de Europa para la protección de los niños contra la explotación y los abusos sexuales, acordada en Lanzarote el 25 de octubre de 2007.
8. En este sentido, véase especialmente el art. 1 de la Directiva del Parlamento Europeo y del Consejo de 2000/31/CE del 8 de junio de 2000 relativa a algunos aspectos jurídicos de los servicios de la sociedad de la información, en especial el comercio electrónico, en el mercado interno (Directiva sobre el comercio electrónico), sobre la cual se volverá en *infra*, epígrafe 7.
9. Acerca de la importancia de este paso y sus reflejos en el Derecho penal de la informática, permítase remitir a a Picotti (2004a), y también, en el mismo volumen y del mismo autor (2004 B), pág. 21 y sig. En la literatura internacional reciente, véase el completo marco crítico, con las correspondientes propuestas de reforma del ordenamiento penal y procesal alemán, delineado por Sieber (2012).
10. Además de mis trabajos anteriores, permítaseme mencionar, acerca de esta distinción sistemática, el reciente trabajo de Picotti (2011), pág. 827 y sig., donde se hallan ulteriores referencias bibliográficas.

mo tiempo provocan peculiares problemas de naturaleza procesal, especialmente en lo referente a las modalidades y condiciones de recogida, conservación y utilización de las llamadas pruebas electrónicas.[11]

Limitándose la intención del presente trabajo a las especificidades del «uso y abuso» de las redes sociales es evidente que en estos casos damos por supuesta la utilización de la red Internet, o en cualquier caso de sistemas de redes informáticas conectadas entre ellas, como pone en evidencia su propio nombre. De este modo, los distintos efectos conexos a las conductas de los usuarios y de quien de cualquier modo acceda a las redes o las gestione se colocan en el ciberespacio, integrando potencialmente siempre «delitos informáticos» –ya sea en sentido estricto o amplio– y más precisamente «delitos cibernéticos», que por tanto recaen en el ámbito de la regulación procesal y de cooperación judicial diseñada por el Convenio sobre Cibercriminalidad del Consejo de Europa de 2001 (especialmente el capítulo II, secciones 2 y 3, artículos 14 y sig., y capítulo III, artículos 23 y sig.).[12]

Desde el punto de vista sustancial, es necesario poner de relieve que las modalidades específicas de tales hechos y comportamientos –condicionados por la distinta extensión y accesibilidad a las redes y a cada información, contenido o dato en general, que se suba y «circule» por las redes sociales– pueden ser muy distintas, lo que provoca diferencias que quedan reflejadas en una distinta valoración penal.

Sin embargo, para una primera investigación que quiera poner de relieve de manera especial la incidencia de los «abusos» cometidos contra los derechos fundamentales infringidos o agredidos en este ámbito, más que entrar en el peculiar y poliédrico análisis del variopinto *modus operandi* de los autores de tales delitos, es preferible limitarse a una clasificación sistemática que siga el tradicional parámetro del bien jurídico o interés penalmente protegido, que permite entender mejor los derechos fundamentales afectados y lesionados.

En este orden de cosas, en primer lugar observamos las infracciones de la esfera propia de cada persona estrechamente conectadas con la naturaleza específica de las redes sociales, que teniendo como finalidad la «comunicación» y la «difusión» de informaciones y datos de cualquier naturaleza constituyen en sí mismos, incluso en su «uso» habitual, una fuente potencial de infracciones en este ámbito. Dentro de esta categoría hay que distinguir entre las infracciones contra la *privacy* en sentido estricto, es decir, relativas a las reglas de tratamiento de los datos personales por un lado (epígrafe 3.1), y a la que en Italia se llama la *riservatezza informatica* por el otro –la «inviolabilidad informática»–, que es una noción más amplia, porque comprende toda lesión del derecho a excluir a terceros de determinados datos, espacios y sistemas informáticos, sin que sea necesario que quede afectada la más reducida esfera de los datos personales (epígrafe 3.2).

En un segundo nivel encontramos los delitos relativos a la producción, difusión y uso de material pornográfico o, en cualquier caso, aquellos que castigan de manera adelantada lo que se consideran síntomas de abusos sexuales y del abuso de menores, como es el caso del delito de *child grooming* introducido recientemente en el ordenamiento italiano para dar actuación al Convenio del Consejo de Europa de Lanzarote de 2007, al que dedicaremos nuestra atención más adelante (epígrafe 5).

Tras ello deberemos considerar todo el resto de los delitos que consistan en una manifestación y difusión del pensamiento que se puedan cometer en las redes sociales, como las injurias y calumnias, la instigación a la violencia o al odio racial o a la discriminación de manera más general, la instigación a la comisión o la apología de delitos contra menores, etc. (epígrafe 5).

En cuarto lugar examinaremos las infracciones de los derechos de autor que recaigan sobre obras protegidas puestas a disposición de los usuarios que se hacen circular –a menudo ilícitamente– por las redes sociales, y que constituyen canales de comunicación y difusión fáciles y ampliamente utilizados con esa finalidad (epígrafe 6).

Obviamente las actividades ilícitas que se pueden realizar a través de las redes sociales son numerosas cuando tales redes se utilizan como medio o «ambiente» para la prepa-

11. Véase en la ya amplia literatura en esta materia, además de las indicaciones señaladas en la nota 2, las contribuciones y el material recogidos en el volumen coordinado por Cajani y Costabile (2011).
12. En la doctrina italiana véase Picotti (2008). Más recientes son las contribuciones de varios autores vertidas en Picotti y Ruggieri (coord.) (2011). De manera especial, acerca de los contenidos procesales del Convenio sobre Cibercriminalidad a la luz de su recepción en Italia, véase también Luparia (2009).

ración, organización o realización de cualquier otro delito: desde extorsiones hasta tráfico ilícito de drogas o armas, desde las asociaciones delictivas en el ámbito de la criminalidad organizada y del terrorismo hasta el proselitismo que se dirige a estos fines, como a otros muchos casos de responsabilidad penal por participación en los más diversos tipos de delitos «comunes» (no cibernéticos) prevista en el artículo 110 del Código penal italiano. Pero, como antes hemos anticipado, más que entrar en detalle en todos los posibles casos y modos de realización de delitos cometidos o que se puedan cometer en o a través de las redes sociales, es importante subrayar que –desde el punto de vista de las exigencias de protección de los derechos fundamentales– sus usuarios, además de posibles autores o partícipes, pueden ser con frecuencia víctimas de muchos de los hechos delictivos a los que nos hemos referido.

Efectivamente, la conducta característica de quien participa en una red social es la de ofrecer a los demás participantes en la red sus contactos y sus «propias» informaciones, comprendidas las imágenes y opiniones, preferencias (de tipo cultural, intelectual, deportivo, etc., e incluso aquellas más «sensibles» como las religiosas, sexuales, políticas, etc.). Por decirlo brevemente, cualquier «cualidad» personal y «actividad» llevada a cabo o proyectada en el tiempo libre o en el ámbito deportivo, profesional o de trabajo, en las relaciones privadas y en las sociales, etc., con la finalidad de mostrarlos y ponerlos a disposición de los destinatarios, a menudo incluso dándoles publicidad, extendiendo así el círculo de «amigos», *follower* o «contactos» ulteriores con personas, grupos, asociaciones o entes.

Esta función esencial de circulación y puesta a disposición voluntaria de las informaciones y los datos personales, y de abrirse a la posibilidad de nuevos contactos, accesos, relaciones, etc. con potencial difusión en cadena de todo ello, expone al usuario a múltiples riesgos de ser objeto de «abusos» o, en cualquier caso, de usos ilícitos o al menos no (expresamente) consentidos de sus datos y contactos.

A pesar de la posibilidad de elección entre distintos niveles de delimitación y protección, de revocación y modificación de las distintas «autorizaciones» dadas o adhesiones expresadas, y de la aplicación de las correspondientes medidas de seguridad, los usuarios no controlan de manera completa y permanente la circulación y difusión de los datos que «suben» y de los accesos que consienten o de los que ellos mismos son objeto, entre otras cosas, porque estas tareas se realizan mediante fáciles y rápidas operaciones con el teclado o el ratón. Basta un simple clic sobre un icono que expresa consentimiento o adhesión y se consiente con la condición y definición de un objeto, una duración, una posibilidad de modificación unilateral, etc. que el usuario ni siquiera suele leer y que no acepta de manera consciente cuando se encuentra ante la exigencia inmediata de concluir determinadas operaciones que requieren ese consentimiento o clic de adhesión para seguir con el procedimiento. Ya desde la fase de registro y aceptación de «amistades» y contactos, etc. el usuario se encuentra en una posición de potencial vulnerabilidad o de «autoexposición» a riesgos de abuso.

Añádase que los límites y niveles de autorización y protección son también susceptibles de ser infringidos y evitados por otros usuarios, por terceros extraños (entre ellos, investigadores o autoridades de policía o judiciales que recogen datos o provocan comportamientos ilícitos infringiendo los límites –aún poco definidos– de licitud de tales instrumentos de intervención) o por los propios gestores de la red social con distintas finalidades, a menudo no explícitamente prohibidas pero tampoco declaradas, como por ejemplo el *profiling* del usuario o el envío de publicidad y ofertas comerciales personalizadas al usuario concreto, a sus gustos, orientaciones, preferencias, hábitos de vida, etc., como lo demuestra la experiencia y la casuística de estos años, que de manera fragmentaria se han puesto de relieve en los medios de comunicación.

Por ello, es fácil entender las razones por las que los usuarios y participantes en las redes sociales, además de poder ser autores, a menudo se convierten a su vez en las primeras víctimas de los delitos cometidos en las redes sociales o través de ellas, como lo demuestra trágicamente el llamado *cyberbullying*, que ha llevado en varias ocasiones a trágicos epílogos.[13]

13. Tómese como caso paradigmático el suicidio de A. G., un adolescente romano de quince años «profilado» en términos negativos como homosexual por un grupo de sujetos de su misma edad que eran alumnos de su instituto y «amigos», o mejor dicho, contactos de Facebook, que pusieron en circulación fotos en las que A. G. llevaba pantalones rosas sin mencionar que se trataba de una fiesta de carnaval. Acerca de los peligros de las redes sociales para la identidad personal, y en especial respecto al *cybebullying*, véanse las amplias y completas advertencias que el Garante de la Privacy italiano ofrece desde hace tiempo en www.garanteprivacy.it (*cfr*. a modo de ejemplo las *slides*: *Social network: attenzione agli effetti collaterali*).

3. Los delitos contra la *privacy* y la «inviolabilidad informática»

3.1. Las violaciones penalmente relevantes de datos personales

De manera muy especial, las características de las redes sociales de las que hemos hablado hacen posible (y frecuente) la comisión de delitos relativos al tratamiento y la circulación de datos personales, materia que en Italia está regulada en el llamado código de la *privacy*, aprobado mediante Decreto legislativo de 30 de junio de 2003, número 196 (en adelante: código de la *privacy*). De entre los tipos penales allí previstos, es especialmente relevante el delito de tratamiento ilícito de datos personales, previsto en su artículo 167.

No parece necesario subrayar que el derecho de toda persona «a la protección de los datos de carácter personal que la conciernan» constituye un derecho fundamental reconocido explícitamente en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, proclamada en Niza en diciembre de 2000 (en adelante, Carta de Niza), a la que el artículo 6.1 del Tratado de la Unión Europea (en adelante, TUE) –en su redacción resultante del Tratado de Lisboa del 1 de diciembre de 2009– dio valor jurídico de tratado. El derecho descrito en este artículo 8 es ciertamente innovador respecto al contenido del más general «respeto de su vida privada y familiar» descrito en el artículo 7 de este mismo texto.[14]

Efectivamente, más allá de la especificidad del derecho reconocido en el artículo 8.1 de la Carta de Niza, el mismo artículo, en sus párrafos posteriores, expresa los siguientes principios, a los que la legislación y la jurisprudencia de los Estados miembros deben adecuarse: «2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

El artículo 1 del código de la *privacy* italiano reproduce la formulación del artículo 8 de la Carta de Niza, reconociendo el rango primario del derecho en cuya tutela se inspira el conjunto de su regulación positiva, que se conforma, a su vez, a los principios citados y que pivota sobre una noción muy amplia de «dato personal».

Según la definición contenida en el artículo 4.1.b del código de la *privacy*, este concepto engloba «cualquier información relacionada con la persona física, identificada o identificable, incluso de manera indirecta mediante referencia a cualquier otra información, incluyendo un número de identificación personal».[15] En este concepto caben pacíficamente también imágenes, sobrenombres, *nicknames*, direcciones electrónicas, cuentas y páginas web personales, números y contraseñas de acceso, *tags* (de las que se hablará más adelante) y cualquier otro extremo que pueda hacer referencia a una persona física. Por tanto, cabe en este concepto una parte altamente relevante de los «materiales» y datos que los usuarios vierten diariamente en la red, ya desde el momento en que se registran.

El concepto de «tratamiento» contenido en el artículo 4.1.a abraza una tal cantidad de operaciones que prácticamente incluye todas aquellas que son habituales en una red social,[16] incluidas la «comunicación» y la «difusión», que se encuentran definidas de manera específica y diferenciada en las

14. Hay que señalar a este respecto que la jurisprudencia de Estrasburgo hacía ya tiempo que había reconducido el artículo 8 del Tratado Europeo de Derechos Humanos (TEDH) al derecho a la *privacy*, de modo que la Unión Europea debe ceñirse a tal interpretación, de la misma manera que debe hacerlo el ordenamiento italiano de conformidad con el artículo 117 de la Constitución italiana, según la interpretación ofrecida por las sentencias gemelas de la Corte Costituzionale de 22 y 24 de octubre, número 347 y número 348 respectivamente, en las que se reconoció a la Comisión Estatal de Derechos Humanos (en la interpretación que de esta realice el Tribunal Europeo de los Derechos Humanos de Estrasburgo) el valor de «norma interpuesta» entre la ley ordinaria y la Constitución italiana. Sin embargo, según el artículo 52.3, última parte de la Carta de Niza, tal eficacia jurídica del TEDH «no excluye que el Derecho de la Unión conceda una protección más amplia».
15. Son datos «sensibles» «los datos personales que puedan revelar el origen racial o étnico, las convicciones religiosas, filosóficas o de otro tipo, las opiniones políticas, las adhesiones a partidos, sindicatos, asociaciones u organizaciones de carácter religioso, filosófico, político o sindical, así como los datos personales que puedan revelar el estado de salud y la vida sexual» (art. 4.1.d del código de la *privacy*).
16. La letra a) del apartado 1 del código de la *privacy* define como «tratamiento»: «cualquier operación o complejo de operaciones efectuadas, incluso sin auxilio de instrumentos electrónicos, relativas a la recogida, grabación, organización, conservación, consulta, elaboración, modificación, selección, extracción, comparación, utilización, interconexión, bloqueo, comunicación, difusión, cancelación y destrucción de datos, aunque no se encuentren incluidos en un banco de datos».

letras m) y l) del mismo artículo por su especial relevancia y específica configuración técnica en el ámbito informático y de las redes en general. La primera consiste, en efecto, en «poner en conocimiento datos personales a uno o más sujetos determinados, distintos del interesado [...], de cualquier forma, incluso mediante su puesta a disposición o consulta». Es decir, no es necesario un envío de los datos a terceros a la «dirección» específica de estos, sino que basta con que los datos «se hayan puesto a disposición», por ejemplo colgándolos en la cuenta del usuario en una red social, o mediante un enlace a otras páginas web u otras cuentas en red conectadas (en los términos mencionados) a uno o más «sujetos determinados» o bien difundidos a sujetos «indeterminados».[17]

Según la estructura meramente «sancionadora» del tipo penal del artículo 167 del código de la *privacy*, inmediatamente perceptible, la conducta de «tratamiento» de datos personales (apartados 1 y 2),[18] de la misma manera que aquellas otras conductas, más duramente castigadas, de «comunicación» y «difusión» (apartado 1, segunda parte) –que en sí mismas constituyen una actividad completamente lícita e incluso habitual para los usuarios de las redes sociales (precisamente porque se encuentran comprendidas su uso normal)– únicamente se convierten en penalmente relevantes cuando se realicen «con incumplimiento» de una de las muchísimas y minuciosas normas extrapenales contenidas en el propio código de la *privacy*, a las que se remite expresamente este artículo 167, aparejándoles de este modo duras consecuencias punitivas.

De entre estas normas extrapenales –que técnicamente hay que considerar como integradoras del precepto penal–, tienen especial relevancia aquellas que requieren el «consentimiento» informado del interesado, que deberá tener forma escrita en caso de ser «datos sensibles»[19] (artículo 23, que remite al artículo 13 del mismo código de la *privacy*). Esta ley define al *interesado* como la «persona física a quien se refieren los datos personales».[20] El interesado, ciertamente, está destinado a convertirse con notable frecuencia en víctima del delito que estamos examinando, cometido por otros usuarios, por terceros o incluso por los gestores de las redes sociales, que pueden convertirse en coautores o partícipes (artículo 110 del Código penal italiano) de todos aquellos que contribuyan al «tratamiento» y en especial a la ulterior «comunicación» o «difusión» de datos ajenos sin contar con un consentimiento válido y específico.

Dado que estos datos pueden estar constituidos por imágenes fotos, vídeos y cualquier otro «material» que permita la identificación de la persona, incluidos aquellos escritos que le hagan referencia incluso indirecta, frases pronunciadas y grabadas vocalmente, expresión de opiniones, etc., inmediatamente se pone de relieve la frecuente práctica de «tagear», como se dice en jerga, que consiste en «marcar» este tipo de material con un *tag* que hace referencia a la persona que aparece en la imagen a la que se refiera el material mediante una especie de «etiqueta electrónica» que indica al sujeto que se quiere identificar.[21]

17. Acerca de las nociones en examen –que fueron definidas en estos términos por la legislación italiana en el artículo 1.2.g) y h) de la ya lejana en el tiempo Ley de 31 de diciembre de 1996, número 675–, pero teniendo en cuenta las nuevas formas de comunicación y difusión que permiten las modernas tecnologías de la información y considerando de manera más específica las «redes» telemáticas, permítaseme la referencia a Picotti (1999), pág. 283 y sig. y pág. 314 y sig.
18. Artículo 167 (tratamiento ilícito de datos): «1. Salvo que el hecho constituya un delito más grave, el que, con la finalidad de recabar un beneficio para sí o para otros, o de causar un perjuicio a otro, proceda al tratamiento de datos personales con incumplimiento de lo dispuesto en los arts. 18, 19, 23, 123, 126 y 130, o bien en aplicación del art. 129, será castigado, si del hecho se deriva algún perjuicio, con reclusión de seis a dieciocho meses o, si el hecho consiste en la comunicación o difusión, con la reclusión de seis a veinticuatro meses. 2. Salvo que el hecho constituya un delito más grave, el que, con la finalidad de recabar un beneficio para sí o para otro o de causar un perjuicio a otro, proceda al tratamiento de datos personales con incumplimiento de lo dispuesto en los arts. 7, 20, 21, 22 apartados 8 y 11, 25, 26, 27 y 45, será castigado, si del hecho se derivara algún perjuicio, con la reclusión de uno a tres años». Para un comentario general de la norma, véase Manna (2003). Para una omitida aplicación a un caso de tratamiento de datos personales en internet sin el consentimiento de la persona interesada, véase el comentario crítico de Salvadori (2006).
19. Para el concepto de datos sensibles, véase la nota 15.
20. Así reza hoy el artículo 4.1.i del código de la *privacy* tras la modificación restrictiva introducida por el artículo 40.2.b del Decreto legislativo de 6 de diciembre 2011, número 201, con las modificaciones introducidas por la Ley de 22 de diciembre de 2011, número 214, que ha excluido la mención a entes, asociaciones y personas jurídicas anteriormente existente.
21. Técnicamente, en informática *tag* significa «término asociado a un contenido digital para facilitar su indexación por parte de los motores de búsqueda» (Wikipedia italiana). En el sitio web italiano de Facebook (http://facebookitalia.blogspot.it) se puede leer: «*Tagear* es una de las acciones fundamentales en Facebook, una de las primeras que es importante entender antes de que sea demasiado tarde y de que

En Facebook, este sujeto debe estar previamente registrado en la red social, y por tanto debe haber «aceptado» (aunque solo en general y en términos abstractos) una tal actividad por parte de los demás usuarios. Sin embargo, no se le pide ningún tipo de consentimiento específico previo a cada *tag* del que sea objeto para que pueda expresar ese consentimiento de manera «informada». En esta red –aunque no solo esta– se promueve, regula y valoriza la actividad de *tagear* por parte de los usuarios, ya que expande y hace circular de manera formidable la «presencia», visibilidad y actividad de los participantes de las redes sociales, que alcanza también las de aquellos que no han señalado o cargado material en su cuenta personal. Por otro lado, mientras que el autor de la foto debe autorizar a un tercero a que cuelgue un *tag* sobre ella, el interesado que es objeto del *tag* solo recibe un aviso en su cuenta y se le da la posibilidad de «destagearse». El problema es que durante el lapso de tiempo que tarde en hacerlo la indexación y los respectivos contenidos que se le han asociado ya han circulado por la red social, y eso puede ocurrir durante mucho tiempo, en el curso del cual tendrán una difusión no delimitable de manera previa e imposible de impedir a posteriori. Este hecho se torna ciertamente problemático cuando el *tag* no corresponde a la efectiva, completa, actualizada, o simplemente más compleja actividad, situación o expresión de la persona «tageada», con lo que se infringen de este modo los requisitos que deben cumplir los datos personales objeto de tratamiento establecidos en el artículo 11, especialmente en sus apartados c) y d), del código de la *privacy*,[22] cuya infracción queda sancionada penalmente de manera expresa mediante la remisión que a ellos hace el artículo 167.3 del mismo código.

Por otro lado, en el caso de sujetos externos a la red social que no tengan una cuenta a la que hacer referencia y que aparezcan, por ejemplo, en una fotografía, vídeo, texto o un diario subido a la red por un usuario, el «tratamiento» de los datos personales y «materiales» que a ellos se refiera (incluido el añadido de un *tag*) se realiza habitualmente sin que exista ningún tipo de consentimiento, comunicación o información al interesado.

Es evidente, por tanto, la enorme cantidad de conductas y hechos que, al menos en abstracto, pueden cumplir con los elementos objetivos del tipo penal que estamos examinando, respecto a los cuales es ciertamente escasa la delimitación que puede ofrecer el elemento del dolo necesario para su punibilidad. A pesar de requerir que concurra una «voluntad consciente» de tratar los datos sin los requisitos y los presupuestos prescritos por la ley –de manera particular sin el previo consentimiento específico e informado del interesado–, es difícil imaginar un convencimiento erróneo de que tales requisitos se den, y especialmente de que el consentimiento del interesado se haya prestado, ya que es irrelevante el error que no recaiga sobre el «hecho»[23] y por el contrario recaiga sobre el precepto penal y su alcance preciso, que viene integrado –como se ha dicho– por las normas extrapenales a las que expresamente reenvía. Yendo a formar parte de este precepto, estas normas extrapenales

podamos cometer alguna metedura de pata, o de que alguien cometa una metedura de pata en nuestro perjuicio de manera impune. *Tag* significa etiqueta en inglés. En el lenguaje de Facebook significa certificar que en una foto (o, desde hace algún tiempo, en una nota de texto) se encuentra presente un determinado usuario de Facebook, que será elegido de la lista de nuestros contactos. Precisamente por eso podemos *tagear* oficialmente solo a nuestros contactos. Oficialmente, significa incluir un enlace al perfil de la persona en cuestión en la página de la foto o de la nota. Al usuario autor de la foto se le pedirá que apruebe el *tag*. En el caso de la foto, también es posible atribuir al usuario en cuestión una posición dentro de la composición. El *tag* es fundamental para enriquecer el número de las fotos que nuestro perfil dirigirá a la voz "foto de". Aparte de las fotografías que nosotros mismos hemos cargado, de hecho, sin la función *tag* no sería posible llegar a una lista completa de fotos de nosotros mismos disponibles en Facebook en los múltiples álbumes ajenos en que aparecemos».

22. El artículo 11, titulado «Modalidades del tratamiento y requisitos de los datos», reza como sigue: «1. Los datos personales objeto de tratamiento son: a) tratados en modo lícito y de manera correcta; b) recogidos y grabados para una finalidad determinada, explícita y legítima, y utilizados en otras operaciones de tratamiento en términos compatibles con esa finalidad; c) exactos y, si es necesario, actualizados; d) pertinentes, completos y que no se excedan de la finalidad para la que se han recogido o hayan sido tratados; e) conservados de modo que permitan la identificación del interesado por un periodo de tiempo no superior al necesario para la finalidad para la que se han recogido o posteriormente tratado. 2. Los datos personales que se traten infringiendo la normativa relevante en materia de tratamiento de datos personales no podrán ser utilizados».
23. Si se tratase de un error culposo sobre un elemento esencial del hecho constitutivo del delito no generaría ningún tipo de punibilidad a título de culpa, ya que según el artículo 47 del Código penal italiano la ausencia de previsión legal del respectivo delito culposo lo impide (aunque deja a salvo la acción de resarcimiento en la vía civil por los posibles daños derivados del tratamiento ilícito, según las reglas de los artículos 15 del código de la *privacy* y 2050 del Código civil.

asumen naturaleza de «ley penal» a los fines de juzgar la inexcusabilidad de la ignorancia (o erróneo conocimiento) previsto en el artículo 5 del Código penal, salvo en los excepcionales casos de ignorancia o error «inevitables».[24]

Hay otros elementos que pueden ser importantes a la hora de penalizar una conducta, que delimitan la tipicidad objetiva del delito en examen respecto a la «pura infracción» de los preceptos procedentes de fuentes extrapenales a los que la norma reenvía. De la infracción debe derivarse un «perjuicio» para la víctima, que marca el momento en que se consuma el delito. Por otro lado, tal infracción se debe cometer «con la finalidad de procurar un beneficio para sí o para terceros, y o de causar un perjuicio a otros». Ciertamente, la interpretación del concepto de «beneficio» es tradicionalmente muy amplia, y se extiende a ventajas de cualquier naturaleza, incluso no económico-patrimoniales. Igualmente amplia es la noción de «perjuicio», que no viene delimitada por ninguna calificación. A pesar de ello, puede derivarse una mínima restricción del hecho típico en el caso de ausencia del resultado que consuma el delito y/o de la ausencia del mencionado nexo teleológico (el elemento subjetivo del tipo antes mencionado), que *ab origine* debe sostener la conducta base de «tratamiento ilegítimo», y en especial las conductas de «comunicación» y «difusión» que infringen la normativa administrativa, especialmente si se reconoce –no solo a nivel sustantivo sino también en el momento de la prueba procesal– que la finalidad requerida no se reduce a un elemento puramente psicológico, interno al ánimo del agente, que encaja únicamente en el tipo subjetivo, sino que ya antes incide sobre la tipicidad objetiva al cuestionar que el hecho comporte una lesión del bien jurídico, porque se refiere a un nexo «causal» que debe subyacer objetivamente a la conducta del agente, de modo que esta conducta será sancionable solo en la medida en que sea instrumento para su satisfacción.[25]

Por otra parte, la concreta valoración de la oportunidad de enervación del procedimiento penal en estos delitos no depende de la parte ofendida, pues se ha excluido la normal procedibilidad por «querela»[26] en consideración a la relevancia de primer orden del bien jurídico lesionado que, efectivamente, va ligada a un derecho fundamental. Por tanto, el hecho de que este tipo de conductas sea perseguible solo de oficio crea una situación en la que la «cifra oscura» de delitos realizados sin persecución concreta sea muy elevada.

Por ello, el penalista no puede evitar preguntarse si no hay que revisar, al menos parcialmente, la normativa vigente, ya que la masiva infracción de la ley penal no solo determina la imposibilidad práctica de la persecución procesal que le corresponde, sino que hace evidente una amplia falta de percepción de ilicitud penal de los comportamientos sancionables tanto por parte de las propias «víctimas», que no formulan denuncia, como por parte de los «autores», entre otros motivos porque en hechos análogos los roles podrían intercambiarse convirtiéndose los que habían sido autores en víctimas y viceversa.

El usuario de las redes sociales, especialmente si pertenece al segmento de población juvenil, parece dispuesto a sacrificar una parte importante de sus derechos en materia de *privacy* a cambio de disfrutar de la posibilidad

24. Ello, según lo dictado por la «histórica» sentencia de la Corte Costituzionale de 24 de marzo de 1988, número 346, consultable en *Rivista italiana di diritto e procedura penale*, 1988, pág. 697 y sig. Sobre el empobrecimiento del dolo en los delitos basados esencialmente en la infracción de preceptos o prohibiciones de contenido estrictamente normativo (como ocurre a los delitos en materia de *privacy* aquí tratados), se reenvía en general a las atentas observaciones de Donini (1993), en especial a las pág. 288 y sig. y 298, en que sugiere distinguir entre el núcleo esencial de la normativa extrapenal que, teniendo carácter general, puede ser considerada perteneciente al «significado cultural» del propio precepto (p. ej. la necesidad de autorización de una actividad que de otro modo resultaría ilegal) y las distintas normativas que tengan la sola función de «concretarlo» ante las varias situaciones, respecto a las cuales por el contrario se debería tratar un posible error como error de hecho.
25. Para una lectura de estos tipos penales con particulares elementos subjetivos del tipo –en Italia llamados con «dolo específico»– sobre la que se volverá también más adelante en el epígrafe 4 a propósito del nuevo delito de child grooming, permítaseme una remisión a Picotti (1993).
26. Nota de la traductora: el instituto procesal italiano de la «querela» no se corresponde con el español de la querella. En el caso italiano se trata de una condición de procedibilidad que consiste solo en dar la *notitia criminis*, que no comporta una calificación jurídica de los hechos y no constituye a quien la formula en parte penal, sino que esta solo solicita el resarcimiento civil de los perjuicios originados por unos hechos. La *querela* italiana solo se puede interponer cuando esté expresamente prevista tal posibilidad en el tipo penal correspondiente, de manera que queda excluida en los demás casos. Aquellos delitos para los que no está prevista pueden ser denunciados, pero solo son perseguibles de oficio y nunca a instancia de parte.

de estrechar y extender sus contactos en la red, de hacer circular e intercambiar sus propios datos y materiales y recibir los de los demás. También a cambio de conseguir todo tipo de ventajas –psicológicas o prácticas– derivadas de la extensión y desarrollo de relaciones sociales y de la participación, aunque sea virtual, en una «comunidad», que le ofrece un fácil aprovechamiento de escritos, imágenes, vídeos u obras artísticas prescindiendo de que estén protegidas por derechos de autor (especialmente musicales y cinematográficas), y en general a cambio de la posibilidad de acceder y tener a disposición una enorme cantidad de información de todo tipo en tiempo real y desde todo el amplio abanico de dispositivos portátiles hoy en uso que puedan conectarse en red.

Dejar también en manos del interesado la opción de la perseguibilidad penal podría constituir un correctivo oportuno a esta situación, que contribuiría a evitar que el sistema penal permanezca lejos de lo que «sienten» los destinatarios de la normativa vigente en esta materia y favorecería una más adecuada y concreta compensación de los intereses en potencial conflicto. Sería, por tanto, deseable la introducción de la perseguibilidad mediante «querela»[27] para un conjunto determinado de conductas o «infracciones» contra la *privacy* del individuo que no presenten extremos de gravedad tales que afecten al núcleo esencial de su derecho fundamental a la protección de los datos personales o al de otros usuarios y por ello falte un efectivo interés público. No habría de ser así, por el contrario, en caso de comportamientos fraudulentos o ilegítimos cometidos por terceros extraños, incluyendo entre estos a los investigadores o fuerzas del orden, que traspasen los límites y las garantías fundamentales establecidas por la ley.

3.2. Los delitos contra la «inviolabilidad informática»

Al lado de las infracciones al código de la *privacy* que acabamos de analizar se colocan otras posibles infracciones similares que afectan al bien jurídico «inviolabilidad informática», es decir, al derecho de los individuos a excluir a terceros no autorizados del acceso y del uso de espacios, sistemas o datos informáticos, sin que sea relevante que el contenido de estos sea «personal» o no.[28] Se trata de un derecho de la persona que al igual que la *privacy* se puede recabar del artículo 7 de la Carta de Niza[29] y que el Tribunal Constitucional alemán ha reconducido recientemente al ámbito de los fundamentales «derechos de la personalidad» relativos a la dignidad humana (*Menschenwürde*) reconocida en el artículo 1 de la Constitución alemana (*Grundgesetz*), y relacionado con el precedentemente reconocido derecho a la autodeterminación informativa, a su vez relacionado con los más tradicionales derechos fundamentales como la inviolabilidad de la correspondencia o la del domicilio.[30]

27. Véase la nota anterior.
28. Sobre la afirmación autónoma de tal bien jurídico, que no es posible incluir en la tutela penal del «domicilio» ni siquiera extendiéndose el concepto al de «domicilio informático», según el punto de vista adoptado por la legislación italiana en la fundamental Ley de 23 de diciembre de 1993, número 547, contra la criminalidad informática, que introdujo (en la correspondiente sección IV del capítulo III, título XII de la parte especial) los artículos 615-*ter*, 615-*quater*, 615-*quinquies* del Código penal, permítaseme la remisión a Picotti (2000), pág. 1 y sig., además de a Picotti (2004b), especialmente pág. 80
29. La necesidad de implementar medidas penales para proteger el «domicilio informático» en cuanto a tal la afirmó el Consejo de Europa en la «Recomendación contra la criminalidad informática» de 1989, número R (89) 9, adoptada el 13 de septiembre –que incluyó el acceso ilegítimo en la «lista mínima» de los hechos que incriminar, tal como más tarde confirmó el Convenio sobre Criminalidad de 2001, cit., que ha colocado en el primer lugar entre los delitos contra la «confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos» la previsión contenida en el artículo 2, que los Estados están obligados a incriminar. De manera análoga, véase el artículo 2 de la Decisión marco UE 2005/222/JAI relativa a los ataques informáticos.
30. Bundesverfassungsgericht (Tribunal Constitucional alemán), 27 de febrero de 2008, 1 BvR 370/0 (www.bverfg.de), mediante la que se anula una ley del Land de Renania del Norte-Westfalia de protección del Estado, que permitía a los servicios de inteligencia «poner bajo vigilancia» durante un periodo de tiempo a sectores enteros de comunicaciones en Internet, o bien a la búsqueda activa mediante software específico de informaciones y datos en red y en los ordenadores conectados a esta, que comportaba una gran intrusión en la esfera de inviolabilidad de los usuarios, que incluso podían ser del todo extraños al objeto de la investigación. El Alto Tribunal alemán ha declarado inconstitucionales las normas en cuestión por infracción del artículo 10 de su Constitución (análogo al artículo 15 de la Constitución Italiana en la medida en que garantiza la *inviolabilidad* del secreto epistolar y de las comunicaciones a distancia), sobre el que ha basado el reconocimiento del «nuevo» derecho fundamental a la libertad, seguridad y confidencialidad en la utilización de instrumentos electrónicos de comunicación como manifestación del derecho general de la personalidad basado en el artículo 1 de la Constitución alemana (dignidad de la persona humana: *Menschenwürde*), del que son expresión tanto el derecho inviolable al domicilio (artículo 13 de la Constitución alemana,

En el ordenamiento italiano este «nuevo» derecho encuentra su protección penal en primer lugar en el delito que castiga el acceso ilegítimo a un sistema informático o telemático previsto en el artículo 614-*ter* del Código penal,[31] y en segundo lugar en el delito «prodrómico» de peligro, que anticipa la barrera de la punibilidad, de tenencia u obtención ilegítima de códigos de acceso o palabras clave, previsto en el artículo 615-*quater* del Código penal. A pesar de que este último se castiga con una pena menor, nos hallamos ante un delito público y por ello se puede proceder de oficio a su persecución, naturalmente debido a su potencial peligrosidad hacia sujetos indeterminados. Por el contrario, frente al más grave delito «final» del artículo 615-*ter* se puede proceder mediante «querella»[32] siempre que no concurran las circunstancias agravantes en él previstas, entre las que cabe destacar la contenida en su número 1, que se refiere a los casos en que el autor sea un funcionario público, el encargado de un servicio público, un investigador privado o un encargado del sistema.

En cuanto a la posibilidad de que estos delitos se puedan realizar en las redes sociales, baste decir que es sin duda alguna técnicamente posible el acceso a «espacios informáticos», páginas web o enlaces ajenos sin contar con el consentimiento o contra la voluntad, aunque sea tácita, del titular, por ejemplo haciéndolo para finalidades a las que este no ha consentido, yendo más allá de los límites concedidos, o utilizando o procurándose ilegítimamente contraseñas de acceso (dando lugar así al tipo preparatorio autónomo del 615-*quater* del Código penal, que materialmente puede concurrir con el tipo principal), o bien utilizando las credenciales de acceso que, aunque se tengan de manera legítima, se usen para realizar modificaciones o introducir informaciones, datos o materiales que no han sido queridas ni consentidas por parte del titular del «perfil» o de la cuenta, tengan esos datos o no un contenido «personal».

En estos casos, además del elemento objetivo que sin duda alguna configura el tipo, dado que se trata de sistemas informáticos protegidos mediante «medidas de seguridad» (como mínimo mediante la necesidad de utilizar contraseña u otras credenciales de acceso) y tal como pacíficamente admite la jurisprudencia, el hecho se perfecciona con el simple acceso no consentido a partes específicas o sectores reservados de un sistema, a pesar de que sea perfectamente legítimo introducirse en otras partes o espacios no reservados de aquellos.[33] Por ello, no debería caber duda alguna de que efectivamente se cumple el tipo subjetivo doloso, ya que no es posible realizar esta clase de conductas si no es con intención, o al menos con la voluntad consciente, de quien gestione los accesos o utilice o consiga indebidamente las contraseñas, palabras clave o credenciales de otro, etc., visto que precisamente las medidas de protección y las reglas técnicas de seguridad de los sistemas informáticos imponen una ejecución «deliberada» de los actos típicos necesarios para infringirlas.

Tal como ya hemos anticipado, también en estos casos el usuario de la red social puede ser tanto autor como víctima de los delitos que estamos examinando, lo que no impide que igualmente los puedan cometer terceros extraños que consigan acceder a la red social, por ejemplo, abusando de perfiles de fantasía o mediante otras técnicas más o menos fraudulentas o ilegítimas.

Con referencia a estas últimas, se hace necesario mencionar (aunque no sea posible analizarla en esta sede) la amplia problemática del *phishing*, que consiste en la utilización de técnicas de «ingeniería social» destinadas a sustraer,

que se corresponde con el artículo 14 de la Constitución italiana) y a la «autodeterminación informativa» (*Recht auf die informationelle Selbstbestimmung*), que había sido previamente reconocido por la famosa sentencia de 1983 del mismo Tribunal en materia de *referendum* (BVerfG, 15.12.1983, 1 BvR 209/83 y sucesivas) y que fue posteriormente confirmada por otra sentencia en materia de *data retention* (BVerfG, 2.3.2010, 1BvR 256/08 – www.bverfg.de). Al respecto, véanse Sieber, «Online-Searches in Global Cyberspace: a new Threat for Criminals and for Civil Liberties», en *Computer crimes and cybercrimes: Global Offences, Global answers* (Actas del Congreso de Verona del 27 y 28 de octubre de 2007, en vías de publicación); también Picotti (2011b), además de diversas intervenciones de Flor (2009b) y (2011).

31. Acerca del alcance de este delito, que ha tenido una amplia aplicación y que recientemente ha sido objeto de una importante sentencia del pleno del Tribunal Supremo italiano (Corte Suprema di Cassazione, Sezioni Unite), de 27 de octubre de 2011 (dep. 7 de febrero de 2012), número 4694, baste la remisión a los recientes comentarios –con exhaustivas indicaciones bibliográficas y jurisprudenciales– de Flor (2012) y Salvadori (2012).
32. Véase la nota 26.
33. Al respecto, véase la sentencia del Tribunal de Rovereto de 9 de enero de 2004 (2 de diciembre de 2003), número 343, confirmada también en sede de legitimidad, con nota de Flor (2005), pág. 81 y sig.

mediante engaño o eludiendo la atención de la víctima, las informaciones personales de esta constituidas por números o palabras de identificación, claves de acceso, contraseñas o credenciales varias,[34] especialmente –pero no solo– cuando permitan acceder posteriormente a cuentas de correo electrónico o de redes sociales, cuentas bancarias on-line o cuando de modo más general sean aptas para conseguir informaciones o datos reservados que interesen al autor del delito, en especial cuando estos tengan trascendencia económico-patrimonial, aunque no solo en estos casos.

Bibliografía

CAJANI, F.; COSTABILE, G. (2011). *Gli accertamenti informaticI nelle investigazioni penali: una prospettiva europea*. Milán: Experta Edizioni.

DONINI, M. (1993). *Il delitto contravvenzionale, «Culpa Iuris» e oggetto del dolo nei reati a condotta neutra*. Milán: Giuffrè. (Università degli Studi di Bologna Seminario giuridico).

FLOR, R. (2005). «Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio e lo "jus excludendi alios"». *Diritto penale e processo*. Núm. 1/2005, pág. 81-89.

FLOR, R. (2007). «Phishing, identity theft e identity abuse: le prospettive applicative del diritto penale vigente». *Rivista italiana di diritto e procedura penale*. Pág. 899 y sig.

FLOR, R. (2008). «Realizzare furti di identità tramite tecniche di phishing integra più fattispecie penali e costituisce un "reato transnazionale"» Nota a Tribunale di Milano, sent. 10 dicembre 2007, n. 888. *Rivista di Giurisprudenza ed Economia d'Azienda*. Núm. 4, pág. 143-146.

FLOR, R. (2009a). «Phishing "misto", attività abusiva di mediazione finanziaria e profili penali dell'attività del c.d. "Financial Manager"» Nota a Tribunale di Milano, 29 ottobre 2008. *Rivista di Giurisprudenza ed Economia d'Azienda*. Núm. 5, pág. 120-123.

FLOR, R. (2009b). «Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. *Online Durchsuchung*». *Rivista di diritto penale dell'economia*. Núm. 3, pág. 695-716.

FLOR, R. (2011). «Tutela dei diritti fondamentali della persona nell'epoca di Internet. Le sentenze del *Bundesverfassungsgericht* e della *Curtea Constituțională* in materia di investigazioni a contenuto tecnologico e *data retention*». En: L. PICOTTI y F. RUGGIERI (coord.). *Nuove tendenze della giustizia penale di fronte alla criminalità informatica. Aspetti sostanziali e processuali*. Turín: G. Giappichelli Editore. Pág. 32-49. (E-book en www.giappichelli.it).

FLOR, R. (2012). «L'introduzione abusiva ed il mantenimento non autorizzato in un sistema informatico nella recente sentenza delle Sezioni Unite. "Abuso" dei profili autorizzativi, "abuso" di poteri da parte del pubblico ufficiale e violazione dello *jus excludendi alios*». *Rivista Trimestrale di Diritto Penale Contemporaneo*. Núm. 1.

FLOR, R. (2013). «La tutela penale della propietà intellettuale ed il contrasto alla collocazione ed alla circolazione in internet di opere o prodotti con segni falsi o alterati». En L. BRUNO y C. CAMALDO. *La circolazione e il contrabbando di prodotti contrafatti o pericolosi: la tutela degli interessi finanziari dell'Unione europea e la protezione dei consumatori*. Turín: G. Giappichelli.

34. Sobre la amplia problemática del *phishing* y sus multiformes manifestaciones, se remite al profundo estudio de Flor (2007), que incluye consideraciones de derecho comparado. Para algunos casos en ámbito bancario, véanse las sentencias del Tribunal de Milán de 29 de octubre de 2008, con comentario de Flor (2009a), y de 10 de diciembre de 2007, también con observaciones de Flor (2008).

LUPARIA, L. (ed.) (2009). *Sistema penale e criminalità informatica: profili sostanziali e processuali nella legge attuativa della Convenzione di Budapest sul cybercrime*. Milán: Giuffrè Editore.

HOFFMANN, K. (2012). «Investigations on Social Networks. A german perspective». *Eucrim*. Núm. 3, pág. 137-140.

MANNA, A. (2003). «Il quadro sanzionatorio penale ed administrativo del codice sul trattamento dei dati personali». *Il diritto dell'informazione e dell'informatica*. Núm. 4/5, pág. 727-770. Milán: Giuffrè.

NIETO MARTÍN, A. (2010). *Redes sociales en Internet y "data mining" en la prospección e investigación de comportamientos delictivos*. *Paper* en *UCLM*. <http://www3.uclm.es>

PICOTTI, L. (1993). *Il dolo specifico. Un'indagine sugli «elementi finalistici» delle fatispecie penali*. Milán: Giuffrè. (Facoltà di Giurisprudenza di Teramo della Università Gabriele d'Annunzio).

PICOTTI, L. (1999). «Profili penali delle comunicación illecite via Internet». *Il diritto dell'informazione e dell'informatica*. Núm. 2, pág. 283-330.

PICOTTI, L. (2000). «Voz "reati informatici"». En: *Enciclopedia Giuridica*. Roma: Treccani. Vol. de actualización VIII, pág. 1-36.

PICOTTI, L. (2004a). «Introduzione». En: *Il diritto penale dell'informatica nell'epoca di Internet*. Padua: Cedam.

PICOTTI, L. (2004b). «Sistematica dei reati informatici, tecniche di formulazione legislativa e beni guiridici tutelati». En: *Il diritto penale dell'informatica nell'epoca di Internet*. Padua: Cedam. Pág. 21 y sig.

PICOTTI, L. (2008). «La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale». *Diritto penale e processo*. Núm. 6, pág. 700-723.

PICOTTI, L. (2011). «La nozione di "criminalità informática" e la sua rilevanza per le competenze penali europee». *Rivista trimestrale di diritto penale dell'economia*. Núm. 4, pág. 827-864.

PICOTTI, L.; RUGGIERI, F. (coord.) (2011). *Nuove tendenze della giustizia penale di fronte alla crimnalità informatica. Aspetti sostanziali e processuali*. Turín: G. Giappichelli Editore. (E-book en www.giappichelli.it).

PICOTTI, L. (2011). «Sicurezza informatica e diritto penale». En: M. DONINI y M. PAVARINI (coord.). *Sicurezza e diritto penale*. Bolonia: Bologna University Press. Pág. 217 y sig.

SALVADORI, I. (2006). «Il trattamento senza consenso di dati personali reperibili su Internet costituisce reato?». *Diritto penale e processo*. Núm. 4, pág. 464 y sig.

SALVADORI, I. (2012). «Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni unite precisano l'ambito di applicazione dell'art. 615 ter c.p.». *Rivista trimestrale di diritto penale dell'economia*. Núm. 1-2, pág. 269 y sig.

SIEBER, U. (2012). «Straftaten und Strafverfolgung im Internet. Gutachten C. zum 69 Deutschen Juristentages». En: STÄNDIGEN DEPUTATION DES DEUTSCHEN JURISTENTAGES. *Verhandlungen des 69. Deutschen Juristentages*. Múnich: Verlag C.H. Beck. Vol. 1 (partes A-F), pág. 157 y sig.

SIEBER, «Online-Searches in Global Cyberspace: a new Threat for Criminals and for Civil Liberties». En: *Computer crimes and cybercrimes: Global Offences, Global answers*. Actas del Congreso de Verona del 27 y 28 de octubre de 2007, en vías de publicación.

Cita recomendada

Picotti, Lorenzo (2013). «Los derechos fundamentales en el uso y abuso de las redes sociales en italia: aspectos penales». 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. 76-90. UOC. [Fecha de consulta: dd/mm/aa]
http://idp.uoc.edu/ojs/index.php/idp/article/view/n16-picotti/n16-picotti-es>
DOI: 10.7238/idp.v0i16.1961

Sobre el autor

Lorenzo Picotti
lorenzo.picotti@univr.it

Catedrático de Derecho penal y de Derecho penal de la informática
Università degli Studi di Verona

Web personal http://www.studiopicotti.com

Palazzo di Giurisprudenza, piso 2, despacho 12
Università degli Studi di Verona
Via Carlo Montanari, 9
37122 Verona
Italia