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 applicazzione 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