InDret
REVISTA PARA EL ANÁLISIS DEL DERECHO
WWW. INDRET.COM

Oportunidad criminal, internet y redes sociales

Especial referencia a los menores de edad como usuarios más vulnerables

Javier García González

Universidad CEU-Cardenal Herrera

BARCELONA, OCTUBRE DE 2015

Abstract

Internet y las redes sociales constituyen un medio idóneo en términos de oportunidad criminal. La ausencia de responsables de los contenidos que se introducen o de las actividades que se puedan realizar en ese entorno, el relativo anonimato del usuario y el modelo de privacidad que se está imponiendo –sobre todo entre los jóvenes– facilita y potencia los comportamientos criminales en el entorno virtual. A lo anterior se unen las dificultades de persecución penal, propias de un sistema jurídico que reacciona con lentitud en un escenario que le es ajeno y prácticamente desconocido. Entre ellas, la falta de experiencia social y jurídica en este ámbito; el cambio de paradigma jurídico que supone aplicar las normas vigentes a una población e incluso a un territorio indeterminado, globalizado; los tiempos de reacción desde que aparecen estas conductas hasta que son finalmente perseguidas; la disgregación normativa existente; los paraísos tecnológicos; o la difícil adecuación del derecho de prueba, por citar los más relevantes. Por todo lo dicho, tras analizar los riesgos y las dificultades señaladas, y partiendo siempre de una valoración positiva de estos avances tecnológicos, se proponen algunas medidas que, entiendo, pueden servir para reducir la aludida oportunidad criminal que amenaza, sobre todo, a los menores de edad, por ser los usuarios habituales de internet. Con ello se pretende provocar el debate sobre cuestiones clave como son el anonimato en internet y el valor del consentimiento otorgado por un menor de edad a través de estos canales de comunicación.

Das Internet und die sozialen Netzwerke bieten Gelegenheiten für strafbares Handeln an und eignen sich dabei als Straftatmittel. Das Fehlen von Verantwortlichen für die Netzinhalte und für die durchgeführten Tätigkeiten, eine gewisse Anonymität der Nutzer sowie der unbesorgte Umgang mit Daten aus der Privatsphäre – vor allem durch Jugendlichen – erleichtern und fördern geradezu kriminelles Handeln im virtuellen Umfeld. Dazu kommen Schwierigkeiten bei der Strafverfolgung durch ein Rechtssystem hinzu, das langsam reagiert, weil ihm das Gebiet fremd und praktisch unbekannt ist.Unter diesen Schwierigkeiten lassen sich Folgende hervorheben: der Mangel an sozialer und rechtlicher Erfahrung in diesem Umfeld, ein juristischer Paradigmenwechsel, der sich als Folge der Anwendung von den geltenden Vorschriften auf eine bestimmte Bevölkerung und sogar auf ein unbestimmtes globalisiertes Territorium, der Zeitraum zwischen der Begehung der Taten und ihrer Verfolgung, die Zerstreuung der geltenden Regelung sowie die schwierige Anpassung der Beweisregeln an solchen Konstellationen. Vor diesem Hintergrund und nach der Analyse der aufgezeigten Risiken und Probleme werden stets aus einer positiven Bewertung des technologischen Fortschritts ausgehend Massnahmen vorgeschlagen, die dazu dienen können, die kriminellen Risiken einzudämmen, die vor allem Minderjährigen als regelmässigen Nutzern des Internets bedrohen. Dadurch soll eine Debatte über entscheidende Fragen wie zum Beispiel die Anonymität im Internet und die Wirksamkeit einer über diese Kommunikationswege zum Ausdruck gebrachten Einwilligung der Minderjährigen hervorgerufen werden.

In terms of criminal opportunity, internet and the social networks represent the perfect medium. The lack of people responsible for what can be found or what can be done in this environment, the relative degree of user anonymity and the model of privacy which is being imposed – especially among young people – expedites and favours criminal behaviour in the virtual world. To the above must be added the legal difficulties involved in prosecution, difficulties which are inherent to a legal system that is slow to react in a setting which is alien and practically unknown. These difficulties include the lack of social and legal experience in this field; the change in legal paradigm involved in applying the existing rules to a population and even a territory which is indeterminate and global; the reaction time between the moment when this behaviour appears and when it is finally prosecuted; the existing fragmentation of the regulations; the

technological havens; or the complicated modification of the right to trial, to name the most relevant. After analysing the risks and difficulties involved, and on the basis that technological advance is always positive, some measures are proposed which, I understand, may be of use in reducing the criminal opportunity which is a particular threat to minors, being the most habitual internet users. The aim of this is to promote debate on key issues such as anonymity on internet and the value of consent granted by a minor through these communication channels.

Titel: Gelegenheit zu kriminellem Handeln, Internet und soziale Netzwerke. Spezielle Berücksichtigung Minderjähriger als besonders verletzbare Nutzer.
Title: Criminal opportunity, internet and social networks. Special reference to the minors like more vulnerable users.

Palabras clave: internet, redes sociales, derecho penal, privacidad, anonimato, oportunidad criminal, validez del consentimiento, menor de edad, adolescente.
Stichworte: Internet, soziale Netzwerke, Strafrecht, Privatsphäre, Anonymität, Gelegenheit zu kriminellem Handeln, Wirksamkeit der Einwilligung, Minderjährige, Jugendliche.
Keywords: Internet, social networks, criminal law, privacy, anonymity, criminal opportunity, value of consent, minor, adolescent.

Sumario

1. Introducción

Hablar de delincuencia, internet y redes sociales supone un reto de síntesis difícil de superar. Para centrar la cuestión sería necesario determinar a qué delincuencia nos vamos a referir con los términos 'cibercrimen'[1], 'cibercriminalidad', 'delincuencia informática', etc.[2]; además, esta problemática suele enlazarse con diversas propuestas de tipología delictiva que muestran la diferencia entre lo que podría denominarse delincuencia tradicional que hace uso de los nuevos medios tecnológicos y –por otro lado– aquellos comportamientos delictivos realmente novedosos que han surgido al abrigo del acceso universal a las tecnologías informáticas[3].Todo ello sin olvidar las complejas cuestiones sobre competencia normativa y jurisdiccional, entre otras, que habrían de aplicarse a una actividad que no conoce fronteras ni tiene una única ubicación geográfica.

Sobre estas cuestiones se ha escrito mucho y bien, por lo que ahora no pretendo incidir en ellas. El objetivo que persiguen estas páginas es el de identificar (alguno de) los riesgos que presenta internet y la participación en redes sociales para el usuario, como potencial víctima de un delito[4]. Y, por ende, las oportunidades que ofrece al delincuente.

De lo anterior podría deducirse una valoración negativa o catastrofista de estas herramientas

[1] Un detallado estudio del origen y significado de este concepto y sus implicaciones jurídicas y criminológicas en los completos trabajos de los Profesores MIRÓ y AGUSTINA. Sin ánimo de ser exhaustivo, cabe citar MIRÓ LLINARES, «La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen», *RECPC,* (13), 2011, pp. 1 ss.; EL MISMO, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, 2012; EL MISMO, «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio», *REIC*, (11), 2013, pp. 5 ss. Y dentro de ese mismo grupo de investigación, la tesis de GARCÍA GILABERT (*Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio*, 2014). Por otro lado, AGUSTINA SANLLEHÍ, «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», *CPC*, (3), 2014, pp. 143 ss.; EL MISMO, «Understanding Cyber Victimization: Digital Architectures and Disinhibition Effect», *International Journal of Cyber Criminology*, (9), 2015, pp. 35 ss.

[2] CRUZ DE PABLO, ya en 2006, afirmaba que la propia mutabilidad de los avances tecnológicos y la aparición de nuevas formas delictivas que, fruto de esa propia mutabilidad, tienen como medio o fin, la informática, hacen necesaria una constante y pormenorizada revisión de las citadas definiciones, pues la que hoy puede considerarse actual quedará absolutamente obsoleta como consecuencia de la inaudita velocidad con la que se producen los avances en el plano de las nuevas tecnologías. Vid. CRUZ DE PABLO, *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, 2006, p. 21.

[3] Asumo la clasificación propuesta por VELASCO. El autor agrupa las diversas conductas delictivas que pueden realizarse en o a través de internet en tres grandes categorías: ciberdelincuencia económica, ciberespionaje o ciberterrorismo y, en tercer lugar, lo que denomina ciberdelincuencia intrusiva (*Delitos cometidos a través de internet. Cuestiones procesales*, 2010, p. 41). Sobre esta última se centra el análisis que hago en este trabajo.

[4] Existen gran cantidad de estudios y datos que analizan la relación entre usuarios de internet y el riesgo de victimización. Cabe citar, entre otros muchos, los siguientes trabajos y/o informes: GARCÍA GILABERT, *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio*, 2014, pp. 6 ss.; DURÁN/MARTÍNEZ-PECINO, «Ciberacoso mediante teléfono móvil e internet en las relaciones de noviazgo entre jóvenes», *Revista Científica de Educomunicación*, (44), 2015, pp. 159 ss.; GIMÉNEZ GUALDO, *Cyberbullying: análisis de su incidencia entre estudiantes y percepción del profesorado*, 2015; GARCÍA FERNÁNDEZ, *Acoso y ciberacoso en escolares de primaria: Factores de personalidad y de contexto entre iguales*, 2013, pp. 64 ss.; CATALINA GARCÍA/LÓPEZ DE AYALA/GARCÍA JIMÉNEZ, «Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet», *Revista Latina de Comunicación Social*, (69), 2014, pp. 462 ss.; DÍAZ-AGUADO JALÓN/MARTÍNEZ ARIAS/MARTÍN BABARRO, «El acoso entre adolescentes en España. Prevalencia, papeles adoptados por todo el grupo y características a las que atribuyen la victimización», *Revista de Educación*, (362), 2013, pp. 348 ss.; TORRES ALBERO/ROBLES/DE MARCO, *El ciberacoso como forma de ejercer la violencia de género en la juventud. Un riesgo en la sociedad de la información y del conocimiento*, 2014.

tecnológicas por mi parte. Nada más lejos de la realidad. Se trata, tan solo, de conocer mejor el hábitat (virtual) en el que 'viven' la práctica totalidad de nuestros jóvenes[5]. De hecho, "poco importa ya el porcentaje (siempre en aumento) de los menores que son usuarios de una o varias redes. (…) Si los adultos vivimos '**con**' internet, los y las jóvenes viven '**en**' internet". Esta, es la gran diferencia que debemos subrayar: lo que para nosotros es una herramienta de alcance e importancia extraordinarios, para ellos y ellas es una forma de vida. Es algo tan cotidiano que "ya es '**su**' forma de vida"[6].

2. Riesgos en internet y en las redes sociales

2.1. Internet como fuente de riesgo

Internet y las aplicaciones en forma de redes sociales que nos ha proporcionado la informática constituyen verdaderos hitos de progreso tecnológico y social. Y como tales son irrenunciables. Ahora bien, lo anterior no impide reconocer que esas mismas herramientas poseen un potencial uso criminógeno nada desdeñable y al alcance de cualquiera.

Precisamente, como indica ROMEO CASABONA, "esta es una de las debilidades de las TIC: su vulnerabilidad para convertirse en un instrumento también muy eficaz de agresión a otros derechos fundamentales"[7].

Por otro lado, los trabajos de MIRÓ LLINARES sobre las oportunidades criminales que ofrece el ciberespacio confirman estas afirmaciones. Este autor enumera y analiza los caracteres intrínsecos y extrínsecos del espacio virtual a tener en cuenta en este sentido[8]. Entre los primeros, apunta el impacto de las coordenadas de tiempo y espacio. También señala cómo, "por una parte, se comprimen las distancias y el tiempo que cuesta recorrerlas; por otra, y derivado de lo anterior, se expanden las posibilidades comunicativas entre las personas y los efectos de los hechos que apenas se ven limitados espacial o temporalmente"[9]. Como es obvio, lo dicho multiplica de forma exponencial las 'incursiones' que puede realizar un potencial delincuente. Además, reduce

[5] Para tener una idea de la dimensión de este medio, es bueno saber que en 2011 alrededor de dos mil doscientos setenta y cinco millones de personas se encontraba conectadas a Internet, representando alrededor del 32,5% de la población mundial (un 70% de población está conectada en los países desarrollados y un 24% en los países en vías de desarrollo). Pero, estamos ante un crecimiento exponencial en el que entre 2000 y 2010 el uso de Internet ha tenido un crecimiento del 444,8%, quintuplicándose el número de usuarios. En Latinoamérica Internet ha penetrado en un 39,5%, mientras en Europa lo ha hecho en un 61,3% y en Estados Unidos y Norteamérica en un 78,6%79 (Estadísticas de International Telecommunication Union, *The World in 2010: ICT Facts and Figures*, http://www.itu.int/ITU-D/ict/statistics/). A su vez, la concentración de usuarios de Internet se encuentra en Asia, que representa el 44.8% de los usuarios mundiales, frente a un 22.1% de Europa, 12 % de Norteamérica, 10.4 % de Latinoamérica y el Caribe, 6.2% de África, 3.4% de Medio Oriente y 1.1% de Oceanía (Fuente Internet World Stats, www.internetworldstats.com/stats4.htm al 31 diciembre 2011). Datos citados por BARINAS UBIÑAS, «El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. Las nuevas formas de ataque a la vida privada», *RECPC*, (15), 2013, p. 17.

[6] PIÑAR MAÑAS, «El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales», en EL MISMO (dir.), *Redes sociales y privacidad del menor*, 2011, p. 62.

[7] ROMEO CASABONA, «Derecho penal y libertades de expresión y comunicación en Internet», en EL MISMO/SÁNCHEZ LÁZARO (eds.), *La adaptación del Derecho Penal al desarrollo social y tecnológico*, 2010, p. 304.

[8] MIRÓ LLINARES, *RECPC,* (13), 2011, pp. 5 ss.

[9] MIRÓ LLINARES, *RECPC,* (13), 2011, p. 10.

en la misma proporción, pero de forma inversa, el esfuerzo que ha de realizar para tratar de obtener sus ilícitos objetivos.

En cuanto a las extrínsecas, tras defender con acierto la relevancia de las mismas a pesar de su naturaleza 'secundaria', incluye la deslocalización, la transnacionalidad (*sic*), la neutralidad y la descentralización del ciberespacio[10]. Nombra de igual modo su carácter universal, popular y anónimo[11]. Y expone cómo, a consecuencia de tales características, el usuario alcanza plena libertad "a la hora de transitar por el mismo sin fronteras, pero también sin censuras por parte de nadie. El carácter neutro de internet deriva de la imposibilidad de bloquear conexiones entre nodos en la red, lo que permite que una vez tengan acceso a internet ni siquiera el propio operador pueda impedir el acceso a una web o a un servicio elegido por el usuario". Esa tecnología, por tanto, nos permite contactar casi en tiempo real con potenciales víctimas y sin riesgo de ser fiscalizado ante la 'ausencia de guardián' alguno[12].

De igual modo, VELASCO NÚÑEZ apunta otros rasgos que vienen a reforzar las apreciaciones anteriores. En su opinión[13], la delincuencia en internet , "aun a riesgo de generalizar", puede describirse con las siguientes notas: son delitos que se cometen a distancia, con plena protección para el agresor y sin posible reacción inmediata de la víctima; de comisión prácticamente instantánea en el tiempo; suelen tener un componente internacional claro (diversa ubicación geográfica del agresor, la víctima y los proveedores de servicio/equipos informáticos implicados); son delitos 'masa' que afectan a numerosas víctimas, con un destacado efecto multiplicador; entre otras.

También destaca otras cuestiones jurídicas no menos relevantes como son la naturaleza menos grave del delito cometido (con los efectos que esto tiene en términos de prescripción penal y posible autorización judicial para enervar los derechos fundamentales afectados); la minoría de edad del autor material (y, por tanto, la activación del régimen jurídico previsto al efecto); el hecho de afectar a múltiples bienes jurídicos, de difusa titularidad; y otras más que terminan por avivar alrededor de internet un potente 'efecto llamada' para delincuentes que encuentran en esta

[10] MIRÓ LLINARES, *RECPC,* (13), 2011, pp. 10 ss.

[11] Sobre este punto se hace hincapié en posteriores epígrafes de este trabajo.

[12] MIRÓ LLINARES, *RECPC,* (13), 2011, pp. 11 y 14. En su opinión (*op. cit.*, p. 21), "han sido las TIC las que han creado el ciberespacio en el que la distancia física deja de ser una barrera infranqueable para muchos delitos, por lo que el ciberespacio se constituye como un ámbito de oportunidad más amplio (siempre en términos potenciales): aumenta considerablemente el número de personas que pueden contactar unas con otras como agresores y objetivos adecuados, expandiéndose, por tanto, el ámbito potencial de oportunidad criminal. En última instancia se trata, por tanto, de que Internet elimina la exigencia de proximidad entre agresor y víctima para la existencia de un delito, con todo lo que ello supone desde una perspectiva preventiva, pero también para la investigación del crimen y el posterior enjuiciamiento del mismo". Profundiza esta propuesta en sus trabajos posteriores, ya citados, *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, 2012, y «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio», *REIC*, (11), 2013, pp. 5 ss. A su vez, desarrolla esta misma propuesta en relación al ciberacoso: GARCÍA GILABERT, *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio*, 2014, pp. 122 ss.

[13] *Delitos cometidos a través de internet. Cuestiones procesales*, 2010, pp. 47 ss. El autor habla igualmente de los problemas que existen para perseguir de forma eficaz a los autores, como son la competencia jurisdiccional, los cortos plazos de prescripción al ser delitos leves, la dificultad de desvelar la identidad del usuario y la vía directa de realización, el lento y tecnificado proceso de prueba que hay que realizar, la dependencia absoluta de la prueba pericial técnica, etc.

herramienta una gran 'ventana de oportunidad criminal'.

En suma, estamos ante un nuevo contexto que presenta unas ventajas evidentes para el agresor frente a su víctima: tiene acceso cualquier persona desde cualquier lugar donde haya una conexión de red y sobre una 'población' en crecimiento exponencial. Todo ello, con mínimas posibilidades de ser detectado, identificado y perseguido por las autoridades de un país que, como sabemos, no tiene por qué ser el mismo en el que reside ni en el que haya llevado a cabo la conducta delictiva. Y entre esas víctimas, también se encuentran los menores de edad, como es obvio[14].

2.2. El modelo de privacidad en internet como riesgo. Especial referencia a los menores de edad

El riesgo que constituye internet para determinados bienes jurídicos dispara su potencial si nos centramos en los ataques realizados sobre la privacidad del individuo. Sin duda, en el campo de la 'ciberdelincuencia intrusiva'[15] el delincuente encontrará a su mejor aliado en la persona del usuario y en el ámbito de las redes sociales a las que éste pertenezca[16].

Quizá la explicación a este fenómeno la podamos hallar en la pregunta que formula RODOTÀ[17]: ¿qué significa vivir continuamente en público, en una dimensión que cancela las fronteras entre la esfera pública y privada, en un flujo continuo de informaciones que cambian la noción misma de identidad?

No por sabido resulta irrelevante que el usuario, de consumidor de información en red, haya pasado a ser creador activo de contenidos en línea. Las aplicaciones que soportan las redes sociales le incitan a ello y son, sin duda, motivo de su gran éxito y aceptación. El propio diseño informático le aboca a exteriorizar información personal a fin de alimentar el funcionamiento de la red social a la que pertenece. Es el conocido 'fenómeno 2.0', que consiste en un cambio de paradigma comunicativo mucho más participativo en el que la diferencia entre emisor y receptor queda ciertamente difuminada.

Por otra parte, si el usuario es el único responsable de administrar su intimidad, la edad con la que puedan acceder a internet y/o a las redes sociales alcanza una gran importancia[18].

---

[14] Con unas características personales y unos hábitos de uso que los hace especialmente vulnerables. Vid. CATALINA GARCÍA/LÓPEZ DE AYALA/GARCÍA JIMÉNEZ, *Revista Latina de Comunicación Social*, (69), 2014, pp. 462 ss.; y GARCÍA JIMÉNEZ/LÓPEZ DE AYALA/CATALINA GARCÍA, «Hábitos de uso en internet y en las redes sociales de los adolescentes españoles», *Comunicar. Revista Científica Iberoamericana de Comunicación y Educación*, (41), 2013, pp. 195 ss.

[15] Incluyendo en esta expresión los ataques a la intimidad, propia imagen, datos personales, secreto de comunicaciones y en definitiva los derechos englobados en el art. 18 CE, como propone VELASCO NÚÑEZ (*Delitos cometidos a través de internet. Cuestiones procesales*, 2010).

[16] En este sentido, consultar el completo análisis que realiza BARINAS UBIÑAS, *RECPC*, (15), 2013, pp. 35 a 54.

[17] «Sociedad contemporánea, privacidad del menor y redes sociales", en PIÑAR MAÑAS (dir.), *Redes sociales y privacidad del menor*, 2011, p. 37.

[18] "Todos los usuarios deben tener en cuenta que son ellos mismos quienes tienen el control respecto a la información y datos personales que desean publicar, por lo que el nivel de responsabilidad respecto de la

En este contexto, se comienza a hablar de 'extemidad' para referirse a la 'involución' que está sufriendo el concepto de intimidad. En opinión de SIBILIA, la raíz interiorista del derecho a la intimidad, tal y como fue concebido hasta ahora, ha cambiado hacia un concepto externo de lo íntimo. Los usuarios, sobre todo los más jóvenes, buscan configurar en la red una personalidad que los defina y distinga frente a los demás. Su perfil social es el medio que usan para ser reconocidos y estimados en ese entorno virtual. Con tales acciones, decae lo introspectivo y se potencia una "externalización de la personalidad". Hasta el punto de entender la pantalla de la computadora, prosigue esta autora, como una ventana siempre abierta y conectada con decenas de personas al mismo tiempo[19]. La misma ventana, por cierto, a la que aludíamos en el epígrafe anterior.

Las variaciones que estos cambios provocan en las relaciones jurídicas son muchas y de gran calado. Por ahora, vamos a destacar únicamente tres de ellas:

Por un lado, la propia tutela jurídica del derecho a la intimidad (en sentido amplio) variará de forma ostensible si varía el objeto formal que le sirve de base, como es lógico. Esto es así porque tal comportamiento no solo produce una 'redefinición' del concepto de intimidad; también modifica el alcance y eficacia de los delitos que pueden ir aparejados a una posible vulneración de ese derecho, como advierte OROZCO PARDO[20]. En este sentido, debemos recordar cómo la jurisprudencia ha ido modelando los contornos de los derechos fundamentales protegidos por el art. 18 CE. En este tiempo, los Tribunales han ido acotando conductas dudosas tales como la grabación oculta y posterior difusión de diálogos o imágenes por parte de uno de los intervinientes en esa conversación y/o escena grabada. También se ha pronunciado sobre la validez procesal de esas grabaciones. Todo ello a fin de otorgarle –o negarle– relevancia penal en relación con el art. 197 CP.

Pues bien, la propia 'tesis del despojamiento de la intimidad' o cualquier otra postura mantenida por el Tribunal Supremo al respecto deberá ahora revisarse/adecuarse ante la 'extemidad' con la que actúa la hipotética víctima de ciberdelincuencia intrusiva. Y lo mismo podrá decirse de las interpretaciones que se hagan respecto de los tipos penales afectados, donde se parte de la protección de la intimidad frente a los poderes públicos y/o terceras personas. Siendo de destacar que en esta ocasión no interviene ninguna otra persona distinta al propio titular de la información difundida.

En segundo lugar, e íntimamente relacionado con lo dicho, habrá que valorar el impacto que el papel de la víctima pueda tener a la hora de incriminar la conducta denunciada. De modo que la duda no recae ya sobre el mayor o menor alcance del tipo penal, como se apunta en el párrafo anterior. Ahora se trata de saber si la norma penal en su conjunto resulta aplicable o si la

publicación excesiva en información y datos puede implicar riesgos para su intimidad" (INTECO-AEPD, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, 2012, p. 166).

[19] Citada por OROZCO PARDO, «Intimidad, privacidad, 'extemidad' y protección de datos del menor ¿un cambio de paradigma?», en BOIX REIG (dir.), *La protección jurídica de la intimidad*, 2010, pp. 390 ss.

[20] En BOIX REIG (dir.), *La protección jurídica de la intimidad*, 2010, p. 393. En su opinión, debemos ponderar que, como alertan los especialistas del foro, internet, las redes sociales y las comunidades virtuales 'debilitan el concepto de intimidad', especialmente en el caso de los menores, que exponen información e imágenes sobre su vida personal de forma voluntaria.

conducta es atípica. En el ordenamiento jurídico español existen precedentes que niegan la protección penal frente a delitos "facilitados" por la propia víctima al omitir una mínima diligencia en su comportamiento previo/coetáneo al delito. Sirva de ejemplo la estafa sobre un inmueble[21]. Nada hace pensar que esto mismo no pudiera ocurrir en el ámbito de los delitos contra la intimidad. Llegado el caso, si la víctima es la que ha compartido toda su intimidad por la red y asume que terceras personas puedan, a su vez, transmitir esa información, ¿se habrá vulnerado su honor, intimidad, propia imagen, secreto a las comunicaciones y/o captación de datos personales? La respuesta no ofrece muchas alternativas, salvo por la edad y madurez de quien así actúa, como luego veremos al tratar del consentimiento.

De hecho, tales cuestiones ya se están planteando ante algunos delitos que ha incorporado el Código penal de 2015. En concreto, MORALES PRATS ha sido muy crítico ante la prohibición de difundir a terceros contenidos íntimos previamente compartidos –de forma voluntaria– entre el sujeto activo y el sujeto pasivo de este delito (art. 197.7 CP)[22]. Junto con los defectos técnicos que, a su juicio, incorpora el texto, dedica severos comentarios sobre la oportunidad y necesidad de elevar estos comportamientos a la categoría de delito. No le falta razón al afirmar que ante la "clara relajación de costumbres en materia de intimidad o, si se prefiere, de una pérdida de las normas de auto vigilancia de esas personas respecto de imágenes íntimas", no se entiende bien por qué el Derecho penal debe prestar tutela a las personas que, libremente, han decidido realizar tales envíos.

Y en tercer lugar (sin que con ello se agote el listado de posibles consecuencias), el concepto de intimidad que rige en internet conlleva, en mi opinión, la aparición de otros peligros para el individuo que lo harán más vulnerable a medio o corto plazo. Peligros de tal relevancia que merecen una adecuada tutela penal.

Sirva de ejemplo la recopilación de los datos personales y vivencias expuestas en la red durante varios años[23]. Si bien es cierto que el art. 18.4º CE incorpora el mandato legal de proteger los datos personales del individuo y los tribunales le otorgan la categoría de derecho fundamental, sigue habiendo mucho por hacer en este terreno. Es más, se llega a afirmar que esa previsión legal "ha reducido los efectos de las nuevas tecnologías sobre los derechos fundamentales a la problemática de las bases de datos". Esto, prosigue ROIG, se debe a dos razones fundamentales. Por un lado, a que la Constitución española es anterior al crecimiento exponencial de internet en los años noventa. Por otro, a que no contiene ninguna cláusula de actualización de derechos fundamentales. De ahí que "los posibles nuevos derechos que aparezcan como consecuencia de la extensión de las nuevas tecnologías de la información y la comunicación no puedan ser

[21] Los Tribunales españoles no dudan en negar la existencia del delito de estafa cuando el comprador no ha consultado el registro de la propiedad para confirmar quién es el verdadero y actual titular del inmueble.

[22] MORALES PRATS, «La reforma de los delitos contra la intimidad. Artículo 197 CP», en QUINTERO OLIVARES (coord.), *Comentario a la reforma penal de 2015*, 2015, pp. 460 ss.

[23] "El usuario debe conocer y considerar las implicaciones que, a nivel profesional, puede tener el hecho de dejar rastros indeseados en este tipo de plataformas, ya que cada vez más, las empresas utilizan este nuevo recurso para identificar posibles candidatos para participar en sus procesos de selección o profundizar en información disponible en el perfil de los candidatos preseleccionados para un puesto de trabajo" (INTECO-AEPD, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, 2012, p. 166).

descubiertos autónomamente por el Tribunal Constitucional"[24].

Con este escenario, de nuevo debemos poner en relación el volcado de datos personales que realiza –¿de forma inconsciente?– el usuario de internet con algunas características de ese entorno virtual: los motores de búsqueda ya son capaces de recuperar en tiempo real cientos de datos, imágenes, referencias, etc.; el denominado 'derecho al olvido', aunque recientemente establecido en Europa[25], tiene mucho camino por recorrer; la regulación en materia de protección de datos suele excluir el tratamiento y recopilación realizado por personas físicas en el ámbito de sus actividades domésticas o personales; no existen aplicaciones técnicas que vinculen una fecha de caducidad cuando introducimos esos datos; la réplica de los mismos en diversos nodos de conexión es una práctica habitual; además, los motores semánticos ampliarán la eficacia de estas búsquedas, entre otras muchas[26].

De lo anterior se concluye que el clásico temor ante un ciudadano 'trasparente' en manos de los detentadores de esa información vuelve a resurgir con más fuerza que nunca[27]. Se habla así de 'dossiers digitales de agregación' o también del 'expediente digital 'de cada uno de los usuarios de internet[28]. E, incluso, se afirma, "con cierta tristeza, que en internet es imposible que se pueda implantar con total seguridad jurídica el derecho al olvido"[29].

Así las cosas, el grado de madurez/edad del usuario que participa en las redes sociales alcanza, como decía, gran relevancia[30]. Tanta que, en mi opinión, deberíamos ponderar la conveniencia de

---

[24] ROIG, «E-privacidad y redes sociales», *Revista de Internet, Derecho y Política*, (9), 2009, p. 43. En el mismo sentido: PICOTTI, «Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales», *Revista de Internet, Derecho y Política*, (16), 2013, pp. 76 ss.

[25] Sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de estos datos (25 de enero de 2012), vid: TRONCOSO REIGADA, «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales», *Revista de Internet, Derecho y Política*, (15), 2012, pp. 61 ss. Sobre los efectos del caso Google, MUÑOZ, «El llamado 'derecho al olvido' y la responsabilidad de los buscadores. Comentario a la Sentencia del TJUE de 13 de mayo de 2014», *Diario La Ley*, (8317), 2014.

[26] Desarrolla algunas de las cuestiones apuntadas: ROIG, *RIDP*, (9), 2009, pp. 42 ss.

[27] Otro buen ejemplo lo encontramos en la recopilación masiva de datos para el reconocimiento facial. El Grupo de Trabajo del art. 29 emitió en marzo de 2012 un dictamen alertando sobre el riesgo para la intimidad de los ciudadanos ante esta técnica de identificación. Vid. DAVARA RODRÍGUEZ, «El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho», *Diario La Ley*, (8158), 2013, p. 5.

[28] Expresiones recogidas en MORENO NAVARRETE, «Aspectos jurídico privados de las tecnologías Web 2.0 y su repercusión en el derecho a la intimidad», en BOIX REIG (dir.), *La protección jurídica de la intimidad*, p. 348. Otros autores hacen referencia a las "huellas digitales" aunque para referirse a las labores de investigación e identificación de los ordenadores utilizados y su recorrido por internet.

[29] DAVARA RODRÍGUEZ, «El derecho al olvido en internet», *Diario La Ley*, (8137), 2013, p. 3.

[30] "No existen restricciones particulares de edad para la utilización de las redes sociales, aunque bien es cierto que la mayoría de las plataformas prohíben el registro de menores de 13 años, recomendando solicitar el permiso de los padres para quienes tienen entre 14 y 18 años. Pero cabe plantearse obviamente cómo puede tenerse la certeza de ello si no existen medios para identificar de forma fehaciente a la persona que suscribe el servicio. (…) El problema también se presenta con menores de entre 14 y 18 años, cuya información se recolecta a partir de la capacidad que, en el mundo virtual, tienen para "permitir" la utilización de sus datos personales con fines comerciales. Menores que se ven expuestos a la configuración de una red que busca, como antes se señalaba, la mayor extracción de información posible sobre sus miembros y que por eso son objeto de campañas publicitarias personalizadas que fomentan el consumismo. Menores que pueden acceder a informaciones no necesariamente aptas para su edad y que se exponen a entrar en un mundo cuyas consecuencias desconocen, seducidos por la inmediatez y rapidez de un ciberespacio en el que "pertenecen" a grupos sin fronteras físicas. Y, cómo no, con

permitir (o no) que sea un menor de edad el que gestione –generalmente sin ayuda alguna– su propio expediente virtual, con todo lo que eso supone a corto, medio y largo plazo. O, en su defecto, acotar la formación y validez de su consentimiento ante actos que van a perdurar durante toda su vida.

2.3. La sensación de 'usuario anónimo' como factor de riesgo

El anonimato en internet desata pasiones. Podría parecer una frase hecha pero resulta llamativa la cantidad de aristas que presenta esta cuestión. A continuación propongo analizar alguna de ellas y resaltar su influencia como factor desencadenante de comportamientos ilegales y/o delictivos.

Como tal, el usuario anónimo en internet no existe. Se podría decir que es una falacia: los ordenadores cuentan con una dirección IP que permite la individualización del terminal desde el que se ha accedido la red. También existen programas que detectan y guardan las 'rutas' por las que hemos navegado de modo que "cuando se utilizan servicios en línea, las personas físicas pueden ser asociadas a identificadores facilitados por sus dispositivos, aplicaciones, herramientas y protocolos". Y esa información, "combinada con identificadores únicos y otros datos recibidos por los servidores, puede ser utilizada para elaborar perfiles de las personas e identificarlas"[31].

Es más, estas 'huellas digitales' son la base esencial del negocio que sostiene la oferta de productos y servicios en internet. Buena muestra de ello son las denominadas 'cookies' y la publicidad personalizada o selectiva que recibe el usuario.

Ahora bien, eso no significa que sea una labor barata, fácil o rápida de realizar. Por otra parte, llegar al terminal supone sólo la mitad de nuestro objetivo: quedaría por conocer la identidad concreta de la persona que lo utilizó.

En todo caso, desde la perspectiva del delincuente esto no es nada nuevo y de seguro que toma las cautelas necesarias para evitar o dilatar su identificación[32]. De hecho, la relativa dificultad técnica para detectarlo se contradice con la casi inalcanzable validez procesal de la información así obtenida y/o la enorme complejidad legal de conseguir, a tiempo[33], una autorización para acceder a los datos de tráfico y/o metadatos que nos lleven hasta el sospechoso.

Por esa razón, la 'sensación' de anonimato que percibe el delincuente constituye el **primer** y principal factor criminógeno de la red: internet minimiza el temor a ser detectado, identificado y detenido. En este sentido, el infractor obtiene una impresión de seguridad por contar con un "refugio aparentemente seguro en el que ocultarse, lo cual, a su vez, le permite reinventarse y

mayores proclives a ignorar y/o menospreciar los riesgos de las redes" (BARINAS UBIÑAS, *RECPC*, (15), 2013, p. 35).

[31] DAVARA RODRÍGUEZ, *Diario La Ley*, (8137), 2013, p. 3.

[32] Siendo que este tipo de delincuentes precisan un conocimiento medio o alto de sistemas operativos informáticos, parece poco probable que desconozcan esta premisa.

[33] Según relata VELASCO NÚÑEZ (*Delitos cometidos a través de internet. Cuestiones procesales*, 2010, p. 93), la necesidad de comisiones rogatorias para solicitar esos datos a empresas con sede en Estados Unidos implica –en ocasiones- que éstas se constituyan y soliciten la información una vez ya haya trascurrido el plazo legal por el que las empresas están obligadas a mantener y custodiar dicha información.

adoptar nuevos personajes virtuales con los que, quizás, cometer delitos"[34]. Se potencia así al "agresor motivado" al que se aludía en páginas anteriores.

Otro **segundo** factor que facilita la delincuencia en el mundo virtual es la propia naturaleza del problema apuntado. Así, plantear una limitación de este anonimato para lograr mayores cotas de seguridad supone una problemática jurídica y social de tal calado, que adoptar una postura equilibrada y consensuada aparece, de inicio, como algo imposible.

De proponerse este debate, aparecerían en cascada los defensores y detractores de los derechos fundamentales a libertad de expresión, a la intimidad, a la protección de datos y secreto de las comunicaciones, entre otros. Se plantearía un debate sobre la democracia real y participativa que propugna la red frente a sistemas políticos tutelados por los propios representantes políticos. Habría sospechas de censura o pérdida de la neutralidad en la red. También se expondrían las propuestas internacionales que tratan la cuestión, tomando como referente la Declaración de Bonn[35], entre otras muchas cuestiones que, por sí solas, justificarían un trabajo de investigación sobre cada una de ellas.

Y, aún en la hipótesis poco probable de alcanzar un acuerdo restrictivo sobre el anonimato, quedaría pendiente su aplicación sobre el terreno concreto. Es decir, habría que contar con mecanismos para que no existieran países desde los que se pudiera acceder sin identificación a la red.

En definitiva, la validez de esos (hipotéticos) logros quedaría condicionada a la inexistencia de 'paraísos informáticos', precisamente, en un mundo que ya está interconectado. Por lo que la propuesta es, sencillamente, inalcanzable (aunque creo que necesaria).

Por otro lado, aun siendo partidario de una identificación segura y encriptada de los usuarios al modo que ya se hace con otros servicios de telecomunicación, es evidente que el 'agresor motivado' no ve riesgos reales que lo pongan en peligro ante una situación como la descrita.

No estamos, en mi opinión, ante una actitud interesada de 'inmovilismo normativo' por parte de las instituciones y/o entidades responsables, como ha ocurrido en otras ocasiones. Más bien, se trata de reconocer la enorme complejidad de alcanzar una regulación –internacional y eficaz– en los cinco continentes[36].

En **tercer** lugar, entre esa oferta de bienes y servicios que se mencionaba existe un nutrido elenco de webs y programas para 'hacerse invisible' en la red. Me refiero a servicios de reenvío anónimo, 'alquiler' temporal de direcciones de correo electrónico, chats y foros donde se accede a

[34] MIRÓ LLINARES, *RECPC,* (13), 2011, p. 25.
[35] En ella se afirma que no se debe incluir ninguna restricción en internet distinta a la que se aplican a otros medios de difusión/comunicación (Declaración del Comité de ministros del CE de 28 de mayo de 2003; sobre libertad de comunicación en internet).
[36] Respecto de cualquier cuestión jurídica, no solo para el Derecho penal. Sirva de ejemplo DIAGO DIAGO, «La residencia digital como nuevo factor de vinculación en el derecho internacional privado del ciberespacio: ¿posible conexión de futuro?», *Diario La Ley*, (8432), 2014.

explicaciones técnicas y enlaces a programas que facilitan la navegación sin rastro, etc.[37]. En definitiva, esos productos existen, son accesibles y hasta podemos recurrir a empresas que se aseguren de que nuestras acciones en red (incluso las delictivas) no dejen rastro. Y difícilmente vamos a poder restringir estos servicios ni prohibir su uso por las mismas razones expuestas.

Si retomamos ahora la perspectiva del usuario, puede decirse que, en muchos casos, esta falsa sensación de anonimato sí constituye una novedad y hasta una contradicción (como ocurre con los menores de edad, por ejemplo).

El usuario se cree anónimo y, por tanto, a salvo de todo tipo de agresiones, incluyendo las delictivas. Esta sensación será en buena parte la responsable de adoptar pocas o ninguna medida de seguridad para prevenir ataques provenientes de otros usuarios. Aunque no incluya su nombre real, no ocultará su verdadero perfil, su estatus social y económico ni tampoco los bienes apreciados o codiciados por terceras personas.

Es más, como decía, resultará hasta contradictorio porque el usuario –que se siente anónimo y actúa protegido con su identidad digital– no tendrá reparo en mentir o, al menos, no aclarar todas las facetas y aspectos de su vida real, a la vez que otorgará plena validez a todo lo que '**está**' en internet, sin realizar unas mínimas comprobaciones al respecto. Incluyendo las afirmaciones de otros usuarios a los que no conoce pero a los que va a otorgarles mayor credibilidad que a cualquier 'guardián' de su entorno familiar o a las directrices emitidas por diversas instituciones para prevenir la delincuencia en internet[38].

Tampoco tendrá inconveniente en visitar webs de contenidos nocivos o inapropiados para su edad, realizar búsquedas de objetos prohibidos o alegales o practicar y difundir comportamientos que nunca llevaría a cabo ni compartiría con terceros si se supiera identificado. Sería el caso del *sexting*[39] o de la piratería musical, por ejemplo.

En suma, se hará mucho más visible en un mundo desconocido y abierto a todos. Y, por tanto, mucho más vulnerable ante posibles ataques contra sus intereses. Por ello, cabría afirmar que la sensación de ciudadano anónimo también puede entenderse como otro factor de riesgo, el **cuarto**, en relación con el cibercrimen.

Pero eso no es todo. Junto con los efectos que genera el anonimato en el agresor y en la víctima, podemos identificar otras consecuencias que quizá comparta cualquier usuario de internet y que también puede influir en la mayor o menor presencia de la delincuencia en el mundo virtual. Me refiero al reconocimiento entre iguales.

---

[37] ROIG I BATALLA, «El anonimato y los límites a la libertad en internet», en COTINO HUESO (coord.), *Libertad en internet: la red y las libertades de expresión e información*, 2007, pp. 321 ss**.**

[38] Como apunta el autor al considerar que los usuarios están expuestos constantemente a la manipulación de la información a través de la tecnología y el alto riesgo de sobre-información (TORRES ALBERO/ROBLES/DE MARCO, *El ciberacoso como forma de ejercer la violencia de género en la juventud. Un riesgo en la sociedad de la información y del conocimiento*, 2014, pp. 37 y 103).

[39] Sobre el fenómeno del *sexting* vid.: MARTÍNEZ OTERO/BOO GORDILLO, «El fenómeno del *sexting* en la adolescencia: descripción, riesgos que comporta y respuestas jurídicas», en GARCÍA GONZÁLEZ (dir.), *La violencia de género en la adolescencia*, 2012, pp. 291 ss. Otros comportamientos igualmente preocupantes son el '*balconing*', '*shokinggame*', '*eyeballing*' o '*car surfing*'.

Al inicio de este trabajo se defendía la bondad de internet y las redes sociales. Afirmación que sigo sosteniendo y que alcanza su mayor exponente en la oportunidad que esta herramienta constituye para colectivos que, por distintas razones, están marginados o padecen algún tipo de limitación. Por ejemplo, no cabe duda que, para quien no pueda moverse de su habitación por motivos de salud, tener una ventana abierta al mundo desde la que contactar con cualquier persona e, incluso, con quienes están en su misma situación, es una bendición. Contribuye a su desarrollo personal y seguramente a su felicidad.

Dicho esto, no debemos olvidar que esa misma herramienta (esa misma ventana), como tantas otras, también puede aprovecharse para fines ilegales. Así, está constatada la existencia de chats, foros y páginas de ayuda para delincuentes, de muy diverso alcance, por no citar el denominado '*deep internet*' o '*deep web*'[40].

Estos hechos –puntuales y por tanto no representativos– deben tenerse en cuenta a la hora de posicionarse ante internet y las redes sociales. Sin exageraciones, desde luego; pero sin olvidar que la asociación criminal sigue vigente en nuestros días y no va a renunciar a ninguna herramienta técnica que facilite la consecución de sus objetivos. Estaríamos, pues, ante el **quinto** efecto negativo que se deriva del mayor o menor grado de anonimato con el que navegamos en internet.

Así pues, a modo de conclusión y con independencia del número real de factores expuesto, considero que el potencial criminógeno del anonimato justifica, en mi opinión, que se reabra un debate sobre dos cuestiones esenciales: 1) regular o no la identificación del usuario de internet; 2) fijar un límite de edad para que los menores puedan acceder a internet (o, al menos, negar hasta cierta edad la validez del consentimiento, tácito o expreso, que esos usuarios puedan otorgar en internet).

Sobre el primero ya he avanzado la casi imposible consecución de solución real alguna. Y tampoco será fácil lograrlo respecto al segundo. Pero no por ello debemos dejar de intentarlo en ambos casos[41].

3. Impedimentos jurídicos que facilitan la delincuencia en internet: el caso español

Tras exponer algunos efectos criminógenos de internet y las redes sociales me centraré ahora en parte de las herramientas jurídicas con las que contamos para luchar contra este tipo de delincuencia. Y debo hacerlo en referencia al ordenamiento jurídico español sin que eso suponga renunciar a la necesidad de pactar una normativa internacional sobre esta materia, más allá de

[40] Se trata de una red no accesible desde navegadores clásicos que opera con el sistema TOR, en referencia a las capas de la cebolla que 'cubren' la identidad real del individuo, en su transcripción inglesa. Se basa en el anonimato de los usuarios, lo que hace mucho más difícil la entrada a la red y la detección de la IP desde la que se accede. Aunque sería incorrecto reducirla, exclusivamente, a contenidos ilegales y delincuencia.

[41] Téngase en cuenta que la identificación previa es obligatoria, por ejemplo, para aquellos mayores de 18 años que quieran participar en juegos online en nuestro país (art. 15 Ley 3/2011, de 27 de mayo, de regulación del juego).

cualquier frontera territorial y jurisdiccional[42].

En concreto, expondré algunas restricciones a las que, a mi juicio, están sometidas esas herramientas jurídicas de modo que impiden o reducen su eficacia; hasta el punto de constituir verdaderos "cortafuegos" que facilitan –en vez de impedir– la propagación de comportamientos delictivos en internet.

3.1. Ausencia de experiencia social y jurídica

Se constata una 'brecha digital' entre las generaciones de los denominados 'nativos digitales' y sus progenitores, con la consecuente ausencia de pautas y experiencia social a las que poder recurrir por parte de padres/tutores para realizar la correspondiente labor de control social informal que estos grupos tienen asignada, como ocurre en otras tantas facetas de la vida. A ello se suma la exigencia y necesidad de que las leyes –y su aplicación en forma de sentencias– se adecúe a los valores y características de la sociedad con la que interactúa[43].

Lo anterior tiene mayores consecuencias de las que, *a priori*, se puedan adivinar. Quizá la más relevante sea el desajuste en las expectativas con las que se va a afrontar el problema y sus posibles soluciones por parte de los actores implicados, en todas sus fases. Y el ordenamiento jurídico español no es una excepción: los tipos penales, las normas procesales, la actuación policial, etc., no pueden cubrir esas expectativas con facilidad porque estamos enfrentando una situación concreta, desconocida hasta ahora, con un cuerpo normativo tradicional, en el sentido más conservador del término.

3.2. Cambio de paradigma jurídico

Reconozco que es una expresión –cambio de paradigma– que se utiliza en muchas ocasiones al hablar de cibercrimen. Quizá en exceso. Pero al añadir el adjetivo 'jurídico' quiero destacar que internet y las redes sociales han forzado una transformación social de tal calado que resultará inevitable que también se transforme el sistema jurídico que lo ha de regular.

No creo que se pueda adaptar la legislación existente, sin más. Tampoco será fácil introducir nuevas normas siguiendo los procedimientos habituales. Si en epígrafes anteriores se ponía de manifiesto la desaparición de los conceptos de 'tiempo' y 'lugar' y su incidencia en el comportamiento criminal, es de suponer que también tendrá efectos en el resto de actores que participan o tienen alguna responsabilidad en el proceso, entre los que ha de incluirse al legislador.

---

[42] Para una perspectiva internacional, el lector encontrará un completo estudio sobre los delitos relacionados con las redes informáticas en las actas del 10º Congreso de las Naciones Unidas sobre prevención del delito y tratamiento del delincuente. En concreto, sobre sus características y tipología, así como sobre los retos que genera en términos de cooperación judicial internacional y de investigación con fines penales (Viena, abril de 2010). Por otra parte, en el 12º Congreso sobre prevención del delito y justicia penal se abordan los retos del 'delito cibernético', insistiendo en la dimensión trasnacional de estos comportamientos y en el posible uso de internet por parte de la delincuencia organizada (Salvador-Brasil, abril de 2010).

[43] Sin que esto pueda interpretarse, erróneamente, con leyes o sentencias que varíen –sin respetar el correspondiente procedimiento formal– conforme lo haga la opinión pública y/o los intereses sociopolíticos de un momento dado. Lo contrario sería negar el principio de legalidad, y no es el caso.

En este sentido, recordar que "el derecho penal y procesal (penal) clásico, así como los principios garantistas inherentes a ambos, han sido construidos, en esencia, sobre la base de un modelo de criminalidad física, marginal e individual"[44] resulta más necesario que nunca.

En otro orden de cosas, aunque comparto la afirmación de que el Derecho siempre ha de ir por detrás de los avances técnicos, con todas sus consecuencias, no es posible mantener los dilatados plazos que los operadores jurídicos se toman para ello. Lo impone la inmediatez de la ciberdelincuencia y el resto de características de internet ya enumeradas. Si eso conlleva la necesidad de recurrir a leyes especiales en vez de usar cuerpos normativos más amplios, como pueda ser el Código penal, habrá que asumirlo.

En 'tiempos' tecnológicos, seguir el proceso tradicional en la creación o modificación de normas penales comporta, en la práctica, asegurar que cuando se adopte el texto legal y entre en vigor ya existirán programas o aplicaciones distintas a las que se pretenda regular o limitar, con el riesgo de ineficacia correspondiente.[45]

Por otro lado, quizá haya que revisar la técnica legislativa con la que se redactan los tipos penales. En el mundo material los actos con relevancia jurídica pueden acotarse con relativa facilidad: las coordenadas de tiempo y lugar son concretas, limitadas, como también lo es la capacidad de movimiento del agresor y el número de víctimas a las que pueda dirigirse. En ese mundo cabe imaginar, como excepción, la acumulación de conductas delictivas y el ataque a diversos bienes jurídicos.

Pero en internet esa excepción será la norma. Además, no se puede reducir la actividad del agresor a una sola y concreta conducta definida en el tipo penal. Buen ejemplo de ello es lo complejo que está resultando castigar la difusión de pornografía infantil virtual, el acecho u hostigamiento y el acoso sexual a menores de edad a través de internet, por citar algún caso. La norma existe, pero la conducta tipificada presenta tantas limitaciones frente a la realizada que a duras penas cumplirá los requisitos típicos. Y aunque éstos se reformulasen y mejorasen, la situación sería parecida ya que la lucha de medios (tecnología-derecho) es desigual por naturaleza[46].

Así las cosas, como dice CRUZ DE PABLO, "la especial naturaleza y forma o modalidad comisiva de los delitos informáticos comporta relevantes dificultades del derecho penal tradicional y de los medios con que cuenta éste, para poder poner fin a determinados comportamientos merecedores de reproche penal. Estas dificultades son precisamente las que dan lugar a la constante aparición

[44] FERNÁNDEZ TERUELO, *Derecho penal e Internet: especial consideración de los delitos que afectan a jóvenes y adolescentes*, 2011, p. 16.

[45] Como ya se ha dicho antes, la difusión no consentida de contenido íntimos remitidos previamente con consentimiento o el embaucamiento de menores para obtener imágenes o vídeos de contenido sexual son comportamientos habituales en internet. Sin embargo, el Código penal español acaba de incorporarlos en julio de 2015.

[46] Sobre estos delitos vid. ALONSO DE ESCAMILLA, «El delito de stalking como nueva forma de acoso. Cyberstalking y nuevas realidades», *La Ley penal*, (105), 2013, pp. 1 ss.; VILLACAMPA ESTIARTE, «El delito de stalking», en QUINTERO OLIVARES (coord.), *Comentario a la reforma penal de 2015*, 2015, pp. 379 ss.; y MATALLÍN EVANGELIO, «Delito de acoso (artículo 172 ter)», en GONZÁLEZ CUSSAC (dir.), *Comentarios a la reforma del Código penal de 2015*, 2015, pp. 575 ss.

de nuevos fenómenos que se encuentran en la delgada línea que separa lo lícito de lo ilícito (…)"[47].

Bien entendido que lo anterior no implica renunciar al principio de legalidad y demás cautelas que limitan el ejercicio del *ius puniendi* por parte del Estado, de las que soy firme defensor. Tan solo –y no es poco– se propugna mayor rapidez y flexibilidad en la creación de tipos penales manteniendo el mismo nivel de seguridad jurídica que en la actualidad[48]. Es, sin duda, un gran reto al que nos enfrentamos para lograr una lucha eficaz frente a una delincuencia 'dinámica', en constante evolución, como también lo es el medio técnico del que se sirve.

3.3. Disgregación normativa

A su vez, en el mundo virtual los sujetos llamados a resolver tales problemas se difuminan entre sí y se agolpan múltiples normas, de diverso alcance y procedencia, que tratan de regular el fenómeno.

Pero lo más preocupante de este proceso, como resalta RODOTÀ, es que esa disgregación, en realidad, genera un "riesgo de recíproca erosión de responsabilidad" de modo tal que no se distinguen con claridad las conductas permitidas de las prohibidas[49]; tampoco se conoce el procedimiento a seguir ni la institución encargada de resolver las posibles reclamaciones[50].

El efecto perverso de esta situación es que los usuarios terminan por identificar la falta de norma o la ausencia de regulación coherente con la permisividad/legalidad de la conducta[51]. Una buena muestra de ello es la piratería musical en internet[52].

---

[47] *Derecho penal y nuevas tecnologías. Aspectos sustantivos*, 2006, p. 76.

[48] Quizá un camino a seguir sea el marcado en el delito de acechanza (de nueva incorporación en el futuro Código penal) y en las causas de atipicidad introducidas en algunos tipos, en concreto, el del *grooming* aunque ésta última adolece, en mi opinión, de una mala técnica legislativa, por la indeterminación o falta de seguridad jurídica que presenta. Se analizan estas cuestiones, aunque en el contexto de violencia de género, en GARCÍA GONZÁLEZ/ESTEVE MALLENT, «La respuesta penal ante la violencia de género en el nuevo código penal español», en ABRIL (coord.), *Mujer, participación política y violencia*, 2015, pp. 326 ss.

[49] En PIÑAR MAÑAS (dir.), *Redes sociales y privacidad del menor*, 2011, p. 38.

[50] "Se recomienda a las autoridades trabajar a favor de un derecho internacional homogéneo en materia de consumidores y usuarios que permita a cualquier usuario o consumidor conocer cuáles son las condiciones mínimas exigibles a cualquier plataforma y que le permitan denunciar cualquier situación que contravenga estos derechos mínimos, con independencia del lugar en el que se encuentre el consumidor, la plataforma y/o donde se haya realizado la transacción (INTECO-AEPD, *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales*, 2012, p. 163).

[51] En parecidos términos, HASSEMER resalta la erosión de las normas sociales. Con este concepto "se pretende aludir al hecho que las expectativas normativas, tales como aquellas que hacen comprensible nuestra cotidianidad, además de estructurarla y asegurarla, han venido reduciéndose claramente". Y prosigue diciendo que "esta erosión no solo ocasiona el entumecimiento de específicos patrones normativos individuales, como los que aclaran y alivianan la cotidianidad (p.ej., la cortesía y la discreción), sino también la reestructuración de indispensables estructuras normativas" (HASSEMER, «El Derecho penal en los tiempos de las modernas formas de criminalidad», en ALBRECHT *ET AL.* (coord.), *Criminalidad, evolución del Derecho penal y crítica al Derecho penal en la actualidad*, 2010, p. 21).

[52] De ahí la importancia de abrir el debate sobre la regulación de internet, como se propone en el texto. En opinión de ROMEO CASABONA, la neutralidad de la red debe ser matizada y "entenderse con un cierto alcance relativo, pues ha de hacer frente a las intervenciones flagrantemente contrarias a los derechos fundamentales y a las libertades públicas" (en EL MISMO/SÁNCHEZ LÁZARO (eds.), *La adaptación del Derecho Penal al desarrollo social y tecnológico*, 2010, pp. 307 y 308).

3.4. Jurisdicción territorial vs. Paraísos tecnológicos

La aplicación territorial de las leyes penales choca con la realidad tecnológica. La delincuencia en internet no conoce estados, fronteras ni territorios definidos. Cierto es que ha habido loables avances en este terreno pero a todas luces resultan insuficientes.

Esto no supone una crítica al trabajo realizado. Todo lo contrario. Pero el cambio de paradigma jurídico que antes reclamaba demuestra su validez en cuestiones como ésta. Nos enfrentamos a un individuo que posee un terminal con acceso a internet y que puede trasladarse de un lugar a otro, sin dejar de interactuar con la red en ningún momento, sin importar el país en el que se encuentra ni tampoco el tiempo que va a tardar en abandonarlo.

Tan es así que aunque la colaboración internacional siga en aumento y se logren grandes avances, seguiríamos teniendo el problema de los tiempos procesales para materializar esos acuerdos de cooperación[53]. Como recuerda BENÍTEZ ORTÚZAR, la inmediatez del resultado y la distancia en la actividad delictiva "obliga a un esfuerzo de los Estados en la cooperación policial y judicial para su persecución, sin la cual, el mejor texto punitivo material sería completamente inaplicable" [54].

Por último queda como problema irresoluble los denominados 'paraísos tecnológicos' donde no existen leyes que limitan estas actuaciones y/o resultan más permisivas que las nuestras. Al respecto tan solo insistir en la diferencia con otras situaciones –aparentemente– similares como pudieran ser los paraísos fiscales: para delinquir en internet no hace falta crear un complejo entramado criminal. Bastaría tener acceso a internet, por cable o por satélite, a través de cualquier dispositivo, desde un territorio sin legislación específica. Incluso podemos automatizar el proceso, como cualquier otra operación realizada por una computadora.

3.5. Validez procesal de las actuaciones de investigación

Como es obvio, el reproche penal dirigido al autor de un delito debe sustentarse en una sólida labor probatoria. El reto, pues, consiste en aportar pruebas que tengan validez en sede judicial. Las mayores dificultades en este sentido son, sin ánimo de exhaustividad, las siguientes:

- En muchas ocasiones es necesaria la **denuncia** de la víctima para iniciar la persecución penal de los hechos. Es el caso de la ciberdelincuencia intrusiva en los que, como regla general, la policía y/o el ministerio fiscal no puede actuar de oficio. Denuncia, por cierto, que deberá hacer la misma persona que, en muchas ocasiones, habrá participado activamente en conversaciones o intercambio de fotos o archivos comprometedores para su intimidad (como sería el caso del *sexting*).

[53] Como relata VELASCO NÚÑEZ (*Delitos cometidos a través de internet. Cuestiones procesales*, 2010, p. 93), al solicitar los datos de tráfico a compañías extranjeras, en su mayoría de USA, es preciso una comisión rogatoria internacional. El problema surge porque, sin duda, ésta se formará y actuará después de haber transcurrido el corto periodo de tiempo durante el que esas compañías están obligadas a conservar tales datos.

[54] «Informática y delito. Aspectos penales relacionados con las nuevas tecnologías», en EL MISMO (coord.), *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, 2008, p. 112.

La cuestión por resolver es si se puede o se debe proteger la intimidad del menor o cualquier otro derecho disponible, contra su propia voluntad[55].

- Aunque ya por poco tiempo, la todavía vigente regulación del **agente encubierto** y la distinción establecida por el TC español entre el delito incitado y el delito descubierto impide que las fuerzas de seguridad se hagan pasar por menores de edad o usuarios para detectar e investigar a presuntos delincuentes. De hacerlo, los datos así obtenidos carecerán, en principio, de valor probatorio.[56]

- Como es sabido, para intervenir la comunicación entre dos personas o para investigar el contenido de una conversación ya finalizada se necesita una **autorización judicial**. Al respecto, el alcance otorgado al art. 18 CE (en sus cuatro apartados) determina qué tipo de autorización ha de emitirse: la que permite enervar el derecho a la intimidad del sospechoso (entrada y registro de su domicilio y enseres que allí hubiera) o la que permite la interceptación de sus telecomunicaciones. Pues bien, dado que los presupuestos legales no son los mismos en uno y otro caso, cualquier decisión errónea al respecto supondrá la nulidad de la prueba obtenida.

  De hecho, la primera (entrada y registro) no resulta suficiente para acceder a las conversaciones de correo electrónico que se estuvieran produciendo en el mismo momento de la entrada a ese domicilio. Tampoco otorga validez, por sí sola, a los denominados 'hallazgos casuales'[57].

---

55 Esta cuestión ya la planteó hace mucho tiempo CORCOY BIDASOLO, «El tratamiento del secreto y el derecho a la intimidad del menor. Eficacia del consentimiento», *Cuadernos de Derecho Judicial*, (12), 1998, pp. 293 ss. En su opinión, el art. 201 CP opta, después de la privatización del impulso del *ius persequendi*, por una fórmula de equilibrio, a través de la cual el Ministerio Fiscal, ponderando los legítimos intereses en presencia, podrá interponer querella. Más reciente, la aportación de RUEDA MARTÍN, «La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la intimidad y la propia imagen. (Especial consideración a la disponibilidad de la propia imagen del menor de edad en el ciberespacio)», *InDret*, (4), 2013, pp. 1 ss.

56 En el tiempo transcurrido entre el envío y publicación de este trabajo, el Congreso acaba de aprobar la reforma de la Ley de Enjuiciamiento Civil y, en concreto, la regulación del agente encubierto. De esta manera, el art. 282 *bis* incorpora los siguientes apartados: "**6**. *El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en comunicaciones mantenidas en canales cerrados de comunicación con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter. El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos.* **7**. *En el curso de una investigación llevada a cabo mediante agente encubierto, el juez competente podrá autorizar la obtención de imágenes y la grabación de las conversaciones que puedan mantenerse en los encuentros previstos entre el agente y el investigado, aun cuando se desarrollen en el interior de un domicilio*".

57 Sobre el alcance de estas autorizaciones judiciales y su incidencia en los derechos fundamentales a la intimidad y secreto de las comunicaciones se pueden consultar diversos trabajos de RODRÍGUEZ LAINZ, «Internet de los objetos y secreto de las comunicaciones», *Diario La Ley*, (8034), 2013; «La interceptación de las comunicaciones telefónicas y telemáticas en el borrador de Anteproyecto de Código Procesal Penal», *Diario La Ley*, (8039), 2013; y «Los límites a la dimensión formal del derecho al secreto de las comunicaciones», *Diario La Ley*, (7669), 2011. En el mismo sentido, ZOCO ZABALA, «Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE», *InDret*, (4), 2010, pp. 1 ss., y GARCÍA SAN MARTÍN, «El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal», *La Ley penal*, (109), 2014, p. 10.

Por lo demás, como es de imaginar, la doctrina[58] y la jurisprudencia[59] no son coincidentes en la materia. Con ello, se generan dudas interpretativas en casos como el acceso, sin autorización judicial, a la agenda de un teléfono móvil no bloqueado; a los datos IP de un ordenador conectado a la red; a los demás metadatos o huellas digitales que deja el dispositivo al navegar por internet; y tantos otros supuestos concretos no previstos en la norma, con el consiguiente riesgo de nulidad procesal de la información así obtenida[60].

- En relación con lo anterior, la naturaleza jurídica de esta clase de **delitos** suele ser la de '**menos graves'** por la pena que tienen prevista. Esa menor relevancia o reproche penal es tenido muy en cuenta por los Tribunales a la hora de conceder las autorizaciones judiciales que afectan a derechos fundamentales del individuo. Reticencias que condicionan negativamente la investigación y castigo de estos delitos (más aun en los que componen la ciberdelincuencia intrusiva).

- Quizá la obligación legal de **conservar datos** durante doce meses parezca suficiente. Pero si se valoran los tiempos procesales, la dependencia técnica en todo este proceso y la necesaria colaboración de empresas de servicios con sede social en el extranjero, los plazos son, a todas luces, insuficientes.

- Por otro lado, no debe confundirse los datos de tráfico y el contenido de la comunicación objeto de investigación (correos electrónicos, por ejemplo) con los contenidos colgados en internet. La legislación española sólo exige la conservación de los primeros y por un tiempo de doce meses desde su divulgación[61]. No existe previsión alguna ni obligación de los proveedores de servicio para que aporten los **contenidos alojados en una página web**. A eso habría que añadir que tampoco resulta fácil lograr la retirada de tales contenidos cuando están albergados en servidores no sometidos a la legislación española[62].

---

[58] Vid. DELGADO MARTÍN, «Derechos fundamentales afectados en el acceso al contenido de dispositivos electrónicos para la investigación de delitos», *Diario La Ley* de 29 de noviembre de 2013.

[59] Entre otras sentencias, vid. AAP Madrid 25 de febrero de 2015, Rec. 39/2015, sobre la investigación tecnológica de delitos cometidos en redes públicas de comunicaciones y la interpretación del término 'delito grave' en La Ley 25/2007. También la STS 26 de noviembre de 2014, Rec. 10269/2014, admitiendo la licitud de la extracción sin autorización judicial de SMS del móvil de una menor fallecida, víctima de una red de prostitución. Sobre la misma cuestión SAN 26 de septiembre de 2013, absolviendo a los responsables de un Centro Educativo que accedieron al móvil de un menor sin la autorización previa de los padres. Sobre el agente encubierto y la cadena de custodia, STS 2222/2013, de 28 de junio, Rec. 11276/2012. Sobre la obtención de la dirección IP y volcado de datos del ordenador, STS 1649/2013, de 26 de marzo, Rec. 10572/2012. Y sobre el registro del listado de teléfonos dentro del móvil, sin autorización del propietario, STS 5170/2011, de 7 de julio.

[60] Ver nota al pie núm. 57.

[61] Aunque el art. 5.2 de la ley 25/2007 de conservación de datos establece alguna excepción y la ley 9/2014 de telecomunicaciones regula en su art. 39 el secreto de las comunicaciones y el acceso a las mismas. Además, a esto hay que unir el conjunto de medidas incluidas en la ley de modificación de la LECrim para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica, que acaba de aprobar el Congreso.

[62] Vid. BARRIO ANDRÉS, «Luces y sombras del procedimiento para el cierre de páginas web: a propósito del desarrollo reglamentario de la 'Ley Sinde'», *Diario La Ley*, (7789), 2012.

- Los requisitos formales para dar validez a las pruebas obtenidas en el registro y clonación de discos duros o cualquier soporte informático son tantos y tan exigentes que romper la **cadena de custodia** por parte de cualquiera de los intervinientes resulta bastante probable. Con esta afirmación no se pone en duda la profesionalidad de los agentes. Se denuncia el exceso de celo que, en mi opinión, se aplica a estos casos desde la perspectiva procesal[63].

- También es compleja la prueba de la autoría en relación con la presunción de inocencia. Al respecto, resulta llamativa la denominada '**teoría de la media electrónica**' por la que se ha dictado una reciente sentencia absolutoria en un caso de fraude económico a través de internet. El Tribunal Supremo reprocha que la investigación no logra despejar la duda razonable de que terceras personas, distintas al sospechoso, pudieran haber usado/manipulado el ordenador desde que se realizó el delito. Al no poder descartar una posible 'monitorización' de ese ordenador, no cabe afirmar –dice el Tribunal– sin margen razonable de duda, que el propietario del mismo fuera, también, quien realizara la conducta delictiva[64]. Postura, sin duda, a tener en cuenta para futuras actuaciones de investigación.

3.6. La indeterminación del régimen jurídico del menor de edad-adolescente

Aunque resulte extraño, el ordenamiento jurídico español no tiene acotado el estatus jurídico del menor de edad. De hecho, podría afirmarse que no define qué debemos entender por tal. Por otra parte, la legislación específica no distingue ni se refiere al adolescente por no ser una categoría jurídica.

Siendo que todas las estadísticas identifican –de forma abrumadora y constante– a los menores y adolescentes como usuarios habituales de internet, se impone conocer con exactitud a quién nos estamos refiriendo y cuáles son sus capacidades legales.

Si bien en la Psicología Evolutiva y en otras ciencias no es un concepto pacífico, por "jóvenes" o "adolescentes" cabría entender personas situadas, aproximadamente, en la franja de entre los 12 y los 18 años y con una capacidad natural superior a la de quienes no han alcanzado esa edad pero a los que todavía no se les reconoce la plena autonomía para gobernarse por sí mismos (reconocimiento que, en términos jurídicos, lograrán tras cumplir los 18 años, como consecuencia directa de ser 'mayores de edad').

Por ello, para el Código penal español, esas personas son "menores", sin más distinción. Lo que sí prevé esta norma es su división en dos grupos, atendiendo a la edad, que da lugar a consecuencias jurídicas bien diferenciadas entre sí: el menor de 0 a 14 años será irresponsable penalmente; mientras que el menor que ya tenga 14 años y no haya superado los 18 tendrá la responsabilidad penal establecida en la Ley penal del menor (en vez de por el Código penal,

[63] Analiza la incidencia práctica de las resoluciones judiciales al respecto: AGUSTINA SANLLEHÍ, «Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia: sobre la garantía del derecho a la intimidad en el registro del ordenador», *La Ley Penal*, (98 y 99), 2012, p. 10.
[64] Comenta esta realidad ANGUIANO JIMÉNEZ, «La teoría de la media electrónica», *Diario La Ley*, (8078), 2013.

reservado a los adultos).

Desde la perspectiva del Código civil la cuestión es igualmente confusa. Los adolescentes tampoco encuentran acomodo, por carecer de reconocimiento jurídico expreso. La legislación civil los tiene por menores de edad a todos los efectos y los sitúa bajo la patria potestad de sus progenitores.

Sin embargo, determinadas leyes (no penales) les reconocen cierta autonomía en la toma de decisiones. También hay relevantes pronunciamientos jurisprudenciales que han supuesto verdaderas 'concesiones' a favor de los adolescentes, aunque sin establecer un criterio claro e idéntico en todos los casos.

En la práctica, esto hace que tengan alguna capacidad legal para gestionar y consentir determinados intereses sin que sea necesaria la intervención de sus padres. Entre ellos, están los derechos "personalísimos", como son los atinentes a su honor, intimidad y propia imagen.

Pero también supone introducir un concepto jurídico indeterminado, sin contornos precisos: es el denominado menor 'maduro'.

Por supuesto, no existe consenso ni definición legal del 'menor maduro', entendiendo por tal a aquél que presenta suficiente discernimiento para gobernarse por sí mismo.

Resultado de todo ello es la figura del menor (individuo que no ha cumplido los 18 años ni se ha emancipado) con muy diversa capacidad de gestión sobre sus bienes y, principalmente, sobre sus intereses, en función de su grado de desarrollo personal.

A estas personas las denominamos adolescentes y/o menores 'maduros', sin duda. Pero no lograremos determinar el régimen jurídico que le es aplicable sin descender al caso concreto, puesto que no dejan de ser menores de edad y de estar –generalmente– bajo la potestad de sus progenitores.

Precisamente ellos, los progenitores, se encuentran al otro lado de la ecuación. Éstos, como regla general, no pueden censurar ni interferir en las actividades de sus hijos (adolescentes) sin más[65]. Ni siquiera pueden hacerlo bajo el 'derecho de corrección' por haber sido desmantelado y derogado del Código civil recientemente.

La razón que lo imposibilita estriba en que la legislación otorga a sus hijos, como se ha dicho, cierta capacidad o autonomía, y ésta solo puede ser retirada y encomendada a los padres o tutores en supuestos excepcionales tasados por la ley (mediante el correspondiente proceso de

[65] Por ejemplo, la STS de 18 de diciembre de 2014 reconoce el derecho de los estudiantes, a partir de 3º ESO, a decidir la inasistencia colectiva a clase sin autorización paterna (en el ámbito de la Comunidad Valenciana) por cuanto son esos estudiantes los titulares del derecho de reunión, siendo inaceptable su ejercicio venga 'condicionado' por una autorización previa expedida por los padres. Otros pronunciamientos sobre los límites del derecho de corrección: SAP Jaén de 22 de enero de 2009, Rec. 9/2009; SAP Asturias de 7 de marzo de 2011, Rec. 18/2011.

incapacitación)[66].

No obstante lo dicho, los progenitores/tutores, son responsables –directos y/o solidarios– de los daños que los menores puedan causar a terceras personas (incluyendo la responsabilidad civil derivada de los delitos que puedan cometer), precisamente, hasta que alcancen la mayoría de edad, al cumplir los 18 años[67].

En resumen, los usuarios de internet y redes sociales (en su mayoría jóvenes o adolescentes, como es obvio) no cuentan con un régimen jurídico definido que le sirva de guía para ellos y/o sus progenitores[68]. Ahora bien, me gustaría matizar esta afirmación porque de lo contrario será objeto de diversas y fundadas críticas.

El adolescente es el único administrador de su privacidad en internet. Comparte y asume un concepto de intimidad al que más arriba se le ha denominado 'extemidad'. Es titular de cuantos derechos fundamentales refleja la Constitución Española, como es lógico. En concreto, lo es del honor, intimidad y propia imagen, en los que no cabe un 'ejercicio por sustitución' al conformar los derechos de la personalidad. Tiene autonomía sexual (aunque limitada) desde los 13 años. Puede ceder sus datos personales (aunque no los del resto de su unidad familiar) a partir de los 14 años, incluyendo fotografías y videos que contengan su imagen en situaciones más o menos comprometidas. Podrá acceder a los sitios webs que considere (más allá de los reservados a los mayores de edad, si es que respeta la 'prohibición'). Podrá contactar e intercambiar información con cualquier otro usuario sin que sus comunicaciones sean filtradas o vigiladas por nadie. Podrá activar herramientas de '*microblogging*' que muestre su ubicación geográfica en todo momento. Podrá usar –en tiempo real– cualquier aplicación informática accesible en red. Y, quizá lo más relevante, podrá otorgar su consentimiento, como de hecho hace cada vez que se descarga contenidos y/o programas en su terminal, sin la presencia de terceros y sin tiempo para reflexionar, más allá de lo que lleve apretar el botón de '*enter*'.

Por otro lado, el padre/madre que –estando atento o preocupado por el uso que haga su hijo/a de esas tecnologías– se encontrará ante un individuo protegido por las leyes, con plena vigencia de sus derechos a la intimidad y secreto de las comunicaciones; que realiza negocios jurídicos eficaces (válidos en términos jurídicos) sin que sea preciso el conocimiento previo de ninguna otra persona; que puede colgar información íntima (incluyendo videos y fotografías) que formarán parte –para siempre– de su "expediente virtual"; que puede consultar y aprender cualquier comportamiento nocivo para su salud y su desarrollo de entre los muchos que tiene a su alcance en las 'bibliotecas virtuales' de su ordenador; que puede acceder a sitios de alto riesgo como es el '*deep web*'; que puede intercambiar experiencias personales –incluyendo claro está las de índole sexual– con desconocidos. En definitiva, un menor que –arrastrado por el sistema web 2.0– interactúa a través de la ventana que se viene nombrando una y otra vez en este artículo;

[66] Además, cuando esto ocurra, las decisiones adoptadas por sus padres/tutores tendrán que perseguir –en todo caso– el 'mejor interés del menor' y presentar las siguientes características: a) estarán dirigidas a una protección integral del menor; b) tendrán una clara finalidad educativa; c) deberán facilitar el libre desarrollo de la personalidad del menor.

[67] Sin olvidar lo dispuesto en el art. 120 CP.

[68] Aunque sí existan diversas leyes que regulan los intereses del menor, como es sabido. Por ejemplo, la reciente L.O. 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia.

como una faceta más de su libertad.

En ese contexto, sería de gran ayuda para todos conocer con detalle el estatus jurídico del menor. Conocer igualmente las herramientas de control que puedan tener los padres/madres. Y, sobre todo, definir expresamente la validez y el alcance que pueda tener el consentimiento que ha prestado de forma telemática un menor de edad, al que quizá también llamemos adolescente, sobre algún aspecto de su vida que quedará integrado para siempre en su dossier digital[69].

4. Algunas propuestas para la discusión

El Derecho penal no debe asumir tareas distintas a las que le corresponden. Por eso sería un grave error usarlo para limitar los avances científicos y/o tecnológicos. Lo mismo podría decirse si se utilizara para dar una imagen –ficticia– de que determinada fuente de riesgo se encuentra bajo control, cuando eso no sea cierto.

En ese doble sentido, se enumera una serie de cuestiones que, en mi opinión, debieran ser objeto de cuidado análisis por incidir de forma directa en la validez de la regulación penal de internet y las redes sociales ante hipotéticos comportamientos criminales. Todo ello, con la única finalidad de reducir riesgos (oportunidades criminales) manteniendo el mayor nivel de libertad y garantías procesales que sea posible.

4.1. Libertad con seguridad

Las reflexiones anteriores se encuadran, desde luego, en el eterno debate sobre el grado de intromisión que debe ejercer el Estado para asegurar las libertades de sus ciudadanos.

Desde la plena confianza en los desarrollos tecnológicos y la defensa de los principios limitadores del *ius puniendi*, entiendo que la sociedad debe perseguir –como meta ideal– el máximo nivel de libertad, sin renunciar a la seguridad necesaria que nos permita disfrutar de ella. No se trata de elegir entre la libertad o la seguridad. Nuestro objetivo ha de ser obtener la máxima libertad con las mejores cotas de seguridad que podamos alcanzar.

No es una ecuación fácil de resolver. Nunca lo ha sido. Pero resulta obvio que esa tarea corresponde a los operadores jurídicos, que no pueden ni deben eludirla.

La identificación remota de los usuarios ¿supone una pérdida de libertad? La respuesta debe darse, en mi opinión, tomando como referencia la libertad que tenemos en la actualidad, cuando navegamos en internet.

[69] En este sentido, RUEDA MARTÍN, *InDret*, (4), 2013. También HERRERA DE LAS HERAS, «El derecho a la propia imagen de los menores de edad ante los medios de comunicación», *Diario La Ley*, (8319), 2014; MACÍAS CASTILLO, «El consentimiento del menor y los actos de disposición sobre su derecho a la propia imagen», *Diario La Ley*, (6911 a 6913), 2008. Y todo ello teniendo en cuenta el respaldo jurisprudencial que estos 'menores maduros' están obteniendo a la hora de ejercer otros derechos fundamentales (vid. NIETO ALONSO, «La relevancia del consentimiento del menor. Especial consideración a la anticoncepción en la adolescencia», *Diario La Ley*, (7041), 2008; y RODRÍGUEZ FERNÁNDEZ, «Novedades jurisprudenciales en Derecho penal de Derecho sanitario», *Diario La Ley*, (8033), 2013. Por último, téngase en cuenta lo dispuesto en el art. 183 *quater* del Código penal de 2015.

En este sentido, no deja de ser curioso que la comunidad virtual acepte la 'vigilancia' a la que están sometidos los usuarios con las '*cookies*' o cualquier otro sistema técnico para identificar nuestras preferencias como consumidores. Lo mismo ocurre con la recopilación ilimitada de datos íntimos hecha desde cualquier motor de búsqueda. Por citar otro caso, el sistema italiano de identificación personal se basa en asignar un número a cada ciudadano pero con la peculiaridad de que dicho número se calcula mediante la combinación de unos pocos datos personales, fácilmente accesibles desde internet. De modo tal que si un individuo conoce o bien el número o bien los datos, logrará identificar al sujeto con relativa facilidad. Lo anterior refleja que nuestra libertad ya sufre importantes restricciones en estos momentos. No se propone ampliarlas. En realidad, se pone el acento, como ya se ha indicado más arriba, en la necesidad de hablar de 'sensación de anonimato' más que de una verdadera identidad oculta. Y dado que esa situación concreta es la realidad en la que nos movemos, también ha de ser, en mi opinión, el punto de partida para valorar estas propuestas.

4.2. Identificación remota del usuario

En mi opinión, debería establecerse la identificación remota de los usuarios mediante sistemas de firma electrónica reconocida o cualquier otro medio similar. Existen recursos técnicos para hacerlo.

Como indicaba en páginas anteriores, reconozco la falta de consenso en este punto y las fuertes resistencias que provoca.

Por el contrario, dejar de ser anónimo no implica convertirse en un ciudadano trasparente. Entre ambos extremos existe mucho trecho por recorrer.

No es necesario –ni se propone– que el usuario interactúe con un identificador que incorpore su nombre completo y la referencia de su número de carnet de identidad. Contamos con medios de encriptación que permitirían una navegación segura y 'reservada' a la vez que facilitaría –solo en caso de ser necesario– localizar los datos personales del usuario. De hecho, esto ya ocurre con las transacciones económicas realizadas por internet, cuando utilizamos un medio de pago de una entidad bancaria: podemos adquirir casi cualquier producto o servicio, incluyendo los que sean poco decorosos o ilegales (servicios sexuales o drogas, por ejemplo). Y no por ello esos usuarios están 'a la vista' de la comunidad virtual ni existen listados de personas identificadas o identificables que realizan tales o cuales comportamientos[70].

Tampoco supondría un límite a la libertad de expresión: la prensa escrita tiene por costumbre incluir el nombre completo del director o responsable de la edición y no por ello podemos decir que se trata de un derecho fundamental cercenado o limitado. Otro tanto ocurre con los titulares de tarjetas SIM para teléfonos móviles sin que por ello pueda afirmarse que sus comunicaciones no son secretas o que no cuentan con toda la protección jurídica que ofrece el Estado de Derecho.

[70] Recuérdese lo dicho sobre la exigencia legal que recae sobre un adulto si quiere practicar una conducta lícita y regulada como es el juego online en España: tendrá que identificarse para poder jugar y las plataformas virtuales realizarán la comprobación en tiempo real sobre su identidad antes de permitir su acceso.

4.3. Grado de madurez/edad del usuario que accede a internet y/o participa en las redes sociales. Valor del consentimiento otorgado por un menor de edad

¿A qué edad debe acceder un menor a los contenidos que ofrece internet? ¿Cuándo podrá gestionar por sí sólo su dossier virtual? ¿Cuántos años debe tener para participar activamente en redes sociales? ¿Prevalece su opinión sobre la de sus progenitores en caso de conflicto?

Desde el punto de vista de la libertad del individuo y el libre desarrollo de su personalidad la contestación a estas preguntas sería bastante fácil. Pero desde la perspectiva de su protección, la respuesta ha de ser más conservadora o limitada.

Atendiendo a la edad penal vigente en nuestro país así como a la autonomía otorgada por la agencia de protección de datos española, parece coherente pensar en la edad de 14 años como límite para que un menor pueda interactuar en internet de forma autónoma[71].

Lo anterior no supone, ni mucho menos, negar el acceso de menores de 14 años a esta herramienta. Son libres de hacerlo. Y espero y deseo que así lo hagan. Pero, en mi opinión, debería establecerse un marco legal según el cual careciese de validez cualquier compromiso ejercitado –en ese contexto– por quien no haya superado esa edad. En todos los niveles. Ese mismo marco jurídico debería aclarar la obligación –y facilitar el derecho– de los progenitores/tutores a intervenir o participar en estas comunicaciones para 'corregir' posibles excesos. De nuevo, no se trata de negar ningún derecho fundamental al menor. Nada más lejos de mi intención. Tan solo se busca una herramienta jurídica que lance un claro mensaje de protección frente a terceros.

Es evidente que internet o las redes sociales no son el 'enemigo'. El menor de esa edad tampoco es el problema. Pero creo que la sociedad en general y los menores en particular necesitan –en mi opinión– recursos ágiles para poder paralizar o reducir los efectos negativos de una mala decisión, que se ha tomado sin suficiente reflexión y/o conocimiento de su verdadero significado.

Cualquier lector tendrá en su memoria conocidos casos de videos de contenido sexual que han comprometido el honor o la intimidad de personajes públicos. Alguno de ellos ha provocado dimisiones y gran escarnio público para los afectados.

Pues bien, sin entrar a valorar el fondo del asunto, considero que un joven al que no se le reconoce plena autonomía sexual (menor de dieciséis años) o al que no se le considera suficientemente maduro como para responder por sus comportamientos delictivos (menor de catorce años), por citar solo dos ejemplos, no debería estar capacitado (legalmente) para hacer lo que quiera en internet. Y mucho menos, para que un tercero –sin identificar– pueda proponerle o

[71] El debate sobre la edad concreta nunca será pacífico porque sobran argumentos para recorrer todo el tramo temporal hasta alcanzar los 18 años. Me inclino por 14 años porque considero que no se puede negar la libertad de acción a quien ya es penalmente responsable de sus actos. Siendo además que la AEPD permite a quienes han cumplido esta edad ceder sus propios datos personales, poco más puede decirse al respecto. Con todo, un buen ejemplo para reflejar la dificultad de saber cuál sería la edad adecuada, es el cambio legislativo que refleja el nuevo código penal respecto a la edad en que un menor puede mantener relaciones sexuales, pasando de 13 a 16 años.

transmitirle cualquier tipo de información o compromiso a través de su terminal de internet. En suma, no creo que esos menores puedan gestionar su dossier digital por sí solos. De ahí que proponga que los tutores/progenitores tengan la capacidad legal reconocida para intervenir ante los proveedores de servicio y/o cualquier otro responsable de contenidos. De forma que –sin necesidad de ninguna otra actuación jurídica adicional– puedan solicitar la retirada de contenidos o el cese de comunicaciones con terceros con la simple demostración documental de ser los tutores/progenitores de un menor de catorce años.

Llegado a este punto, sin duda discutible, creo que la mejor defensa de ésta propuesta es que el lector, de nuevo, responda a las siguientes preguntas: qué tendría que hacer un padre/madre para retirar un video comprometido que haya sido protagonizado y 'colgado' por su propio/a hijo/a en internet; qué facilidades le van a dar los proveedores de servicio; qué cobertura legal obtendrá desde la administración, incluyendo los tribunales de justicia; qué tiempo material transcurrirá desde que 'denuncie' los hechos hasta que se retiren esos contenidos o se logre cerrar la web; etc.

Otro argumento que cabe esgrimir a favor de esta limitación es, precisamente, la posibilidad que brinda para exigir responsabilidades a esos mismos progenitores/tutores en caso de omitir cualquier tipo de control respecto de los menores a su cargo en ese mundo virtual. Al fin y al cabo, tendrían que asumir el mismo deber de cuidado que, en definitiva, les corresponden como en otras tantas ocasiones, dentro del proceso educativo y formativo de sus hijos/as[72].

En coherencia con lo anterior, el consentimiento otorgado por un menor de catorce años a través de internet o redes sociales no debería tener eficacia jurídica si no es corroborado por el progenitor/tutor.

Esto supondría que los proveedores de servicios tendrían la obligación de comprobar la edad del usuario para asegurarse que éstos superan el límite fijado. De no hacerlo, esos mismos proveedores tendrían la responsabilidad legal de buscar y retirar el 'dossier digital' que pudiera haber generado ese menor, en la medida y alcance que permita la técnica del momento.

A su vez, quien intercambiara comunicaciones con un menor de esta edad tendría la certeza jurídica de hacerlo con un individuo especialmente 'protegido', con todo lo que eso conlleva. Se trataría, en suma, de crear una presunción jurídica que favoreciese al menor en caso de conflicto y que amparase las actuaciones de los progenitores/tutores que se dirigieran a ese fin, sin necesidad de una previa y lenta autorización judicial para reconocerles esa legitimidad.

De lo anterior se desprende la necesidad de asumir la identificación remota del usuario antes defendida. También resultaría necesario regular, de forma específica, la obtención del consentimiento de un menor de catorce años en internet, así como el objeto o contenido del mismo, de manera similar a como se hace ya respecto a la cesión de sus datos personales. De

[72] Desde no hace mucho tiempo, el Ministerio Fiscal viene solicitando la imputación de aquellos conductores que sufren un accidente y transportaban a menores de corta edad -a su cargo- y que han fallecido por no comprobar que éstos viajaban con las mínimas medidas de seguridad exigibles.

hecho, bastaría con completar la regulación administrativa que ofrece la LPD en este sentido[73].

4.4. Instrumentos legales adecuados

Con independencia de lo dicho hasta ahora, cualquier protección jurídica eficaz para los usuarios de internet viene comprometida por la validez procesal de las labores de investigación que tengan que realizarse.

En este campo, a pesar de las importantes reformas y avances que se han producido, queda mucho por hacer. Me refiero, por citar alguno de ellos, a la regulación del agente encubierto en internet[74]; al posible uso del delito de acechanza como respuesta legal ante el acoso telemático; a la tipificación de la usurpación de identidad digital, como acaba de proponer la Fiscalía; el hecho de permitir el acceso a los datos de tráfico y al contenido de ordenadores y agendas de contactos, integrando todos ellos dentro del derecho a la intimidad del sospechoso, pero sin el amparo del secreto de las comunicaciones que también le asiste; la validez de los hallazgos casuales, si tiene su origen en una investigación previa autorizada por el juez; entre otras muchas.

Y hacerlo, como también se dijo, ajustando los plazos jurídicos, en la medida de lo posible, con los plazos tecnológicos y asimilando la ausencia de referentes concretos de espacio y tiempo. Sin renunciar, por ello, al rigor garantista de cualquier norma penal.

4.5. Responsabilidad por el diseño del producto

En ningún caso se defiende la responsabilidad penal objetiva desde estas páginas. Los fabricantes de determinados productos no son responsables penales del uso inadecuado que de ellos puedan hacer terceras personas, como es obvio.

Pero también lo es que desde diversas instituciones se viene pidiendo que las aplicaciones informáticas sean respetuosas con la privacidad[75]. Y otro tanto cabría decir sobre el anonimato, impidiéndolo en la medida de lo posible, mediante la introducción de tecnologías que mejoren, por defecto, la seguridad en internet conforme los parámetros marcados por la ley.

En este sentido, y para finalizar, propongo asumir el sistema procesal y la solución legal adoptada en Brasil para luchar contra los ataques contra el honor que, de forma anónima, se

[73] Vid. Informe 0046/2010, Gabinete Jurídico de la AEPD, sobre el tratamiento de datos personales de menores de edad y el Informe 2000/0000, sobre consentimiento otorgado por menores de edad.
[74] Ver nota al pie núm. 56.
[75] En la 30 Conferencia Internacional de Autoridades de Protección de Datos y privacidad se adoptó la resolución sobre protección de la privacidad en los servicios de redes sociales. En ella se pide "configuraciones por defecto que sean respetuosas con la privacidad", que sean "especialmente restrictivas cuando un servicio de redes sociales esté dirigido a menores". De hecho, solicitan que los proveedores tomen medidas eficaces para impedir el las descargas en masa de datos de perfil por parte de terceros así como garantizar que los datos de los usuarios solo pueden explorarse en motores de búsqueda externos a la red social en cuestión cuando hayan dado su consentimiento explícito e informado. En parecidos términos se expresó el Grupo de trabajo sobre protección de datos del artículo 29. En su Dictamen 5/2009 sobre las redes sociales en línea, pide "la instauración de tecnologías que mejoren la protección de la intimidad, es decir, parámetros por defecto respetuosos de la intimidad, ventanas emergentes de advertencia en fases adecuadas, así como programas informáticos de verificación de la edad".

realizaban desde internet, ampliándolo a cualquier clase de ofensa grave contra el ciudadano[76]. La propuesta, como se ha dicho, consiste en hacer responsable al proveedor no por los contenidos que cuelga el usuario, sino por las aplicaciones y programas que proporciona el proveedor y que no permiten la identificación de ese usuario.

Como relata DE GREGORIO[77], el problema de las injurias a través de redes sociales alcanzó gran relevancia en este país. La víctima podía acudir ante las autoridades judiciales para defender su honor, mediante un proceso sencillo, rápido y sin necesidad de abogado.

La empresa responsable del servicio había sido citada en la práctica totalidad de esos procesos para que aportara los datos del usuario-difamador, en calidad de responsable civil subsidiario. Al tratarse de una representación territorial de la empresa norteamericana Google, ésta se negó a entregar tales datos argumentando que no estaba sometida a las leyes brasileñas. Además, consideraba que no podía ser demandada por las acciones injuriosas que realizaban los usuarios a través de su plataforma.

Los jueces brasileños le contestaron negando ambos argumentos. En primer lugar, consideraron que la empresa erala responsable de que la aplicación tecnológica que ofrecía y comercializaba amparara o permitiera el anonimato del usuario. En segundo lugar, porque esa empresa norteamericana contaba con una sede territorial en Brasil que tenía capacidad para aceptar los pagos por los servicios de publicidad y otros ingresos, además de desarrollar una actividad lucrativa en territorio de Brasil y dirigido, principalmente, a los ciudadanos de ese país. Por todo lo dicho, condenaron a Google como responsable civil subsidiario.

Desde entonces, se llegó a un acuerdo entre ambas partes para lograr identificar a los usuarios que realizaban tales conductas, lo que supuso –en la práctica– un fuerte descenso de esas prácticas. Un buen final que deberíamos tener en cuenta.

5. Bibliografía

AGUSTINA SANLLEHÍ (2015), «Understanding cyber victimization: digital architectures and disinhibition effect», *International Journal of Cyber Criminology*, (9), pp. 35 ss.

——— (2014), «Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización», *Cuadernos de Política Criminal*, (3), pp. 143 ss.

——— (2012), «Interrogantes en torno a las diligencias preliminares ante la ciberdelincuencia: sobre la garantía del derecho a la intimidad en el registro del ordenador», *La Ley Penal. Revista de derecho penal, procesal y penitenciario*, (98 y 99), p. 10.

——— (2010), «El debate actual entre privacidad y prevención del delito: una propuesta

[76] Cierto es que la Constitución brasileña prohíbe expresamente el anonimato, cosa que no ocurre en España, como es sabido.

[77] «Niños y adolescentes en las redes sociales: una visión desde América Latina y el Caribe», en PIÑAR *ET AL.* (coords.), *Redes sociales y privacidad del menor*, 2011, p. 273.

comunitarista», *Indret. Revista para el Análisis del Derecho*, (1).

ALONSO DE ESCAMILLA (2013), «El delito de stalking como nueva forma de acoso. Cyberstalking y nuevas realidades», *La Ley penal. Revista de derecho penal, procesal y penitenciario*, (105), pp. 1 ss.

ANGUIANO JIMÉNEZ (2013), «La teoría de la media electrónica», *Diario La Ley*, (8078).

BARINAS UBIÑAS (2013), «El impacto de las tecnologías de la información y de la comunicación en el derecho a la vida privada. Las nuevas formas de ataque a la vida privada», *Revista Electrónica de Ciencia Penal y Criminología,* (15).

BARRIO ANDRÉS (2012), «Luces y sombras del procedimiento para el cierre de páginas web: a propósito del desarrollo reglamentario de la 'Ley Sinde'», *Diario La Ley*, (7789).

BENÍTEZ ORTÚZAR (2008), «Informática y delito. Aspectos penales relacionados con las nuevas tecnologías», en EL MISMO (coord.), *Reforma del Código Penal. Respuestas para una sociedad del siglo XXI*, Dykinson, Madrid, pp. 109 ss.

CATALINA GARCÍA/LÓPEZ DE AYALA/GARCÍA JIMÉNEZ (2014), «Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet», *Revista Latina de Comunicación Social*, (69), pp. 462 ss.

CORCOY BIDASOLO (1998), «El tratamiento del secreto y el derecho a la intimidad del menor. Eficacia del consentimiento», *Cuadernos de Derecho Judicial*, (12), pp. 293 ss.

CRUZ DE PABLO (2006), *Derecho penal y nuevas tecnologías. Aspectos sustantivos,* Grupo Difusión, Madrid.

DAVARA RODRÍGUEZ (2013), «El tratamiento de datos de carácter personal y la utilización de la tecnología: entre la ética y el derecho», *Diario La Ley*, (8158).

———— (2013), «El derecho al olvido en internet», *Diario La Ley*, (8137).

DIAGO DIAGO (2014), «La residencia digital como nuevo factor de vinculación en el derecho internacional privado del ciberespacio: ¿posible conexión de futuro?», *Diario La Ley*, (8432).

DÍAZ-AGUADO JALÓN/MARTÍNEZ ARIAS/MARTÍN BABARRO (2013), «El acoso entre adolescentes en España. Prevalencia, papeles adoptados por todo el grupo y características a las que atribuyen la victimización», *Revista de Educación*, (362), pp. 348 ss.

DURÁN/MARTÍNEZ-PECINO (2015), «Ciberacoso mediante teléfono móvil e internet en las relaciones de noviazgo entre jóvenes», *Revista Científica de Educomunicación*, (44), pp. 159 ss.

FERNÁNDEZ TERUELO (2011), *Derecho penal e Internet: especial consideración de los delitos que afectan a jóvenes y adolescentes*, Lex Nova, Valladolid.

GARCÍA FERNÁNDEZ (2013), *Acoso y ciberacoso en escolares de primaria: Factores de personalidad y de contexto entre iguales*, Servicio de Publicaciones de la Universidad de Córdoba, Córdoba.

GARCÍA GILABERT (2014), *Victimización de menores por actos de ciberacoso continuado y actividades cotidianas en el ciberespacio,* tesis doctoral, Universidad de Murcia.

GARCÍA GONZÁLEZ/ESTEVE MALLENT (2015), «La respuesta penal ante la violencia de género en el nuevo código penal español», en ABRIL (dir.), *Mujer, participación política y violencia*, Huygens Editorial, Barcelona, pp. 295 ss.

GARCÍA JIMÉNEZ/LÓPEZ DE AYALA/CATALINA GARCÍA (2013), «Hábitos de uso en internet y en las redes sociales de los adolescentes españoles», *Comunicar. Revista Científica Iberoamericana de Comunicación y Educación*, (41), pp. 195 ss.

GARCÍA SAN MARTÍN (2014), «El hallazgo casual o descubrimiento ocasional en el ámbito de la investigación penal», *La Ley penal. Revista de derecho penal, procesal y penitenciario*, (109), p. 10.

GIMÉNEZ GUALDO (2015), *Cyberbullying: análisis de su incidencia entre estudiantes y percepción del profesorado,* tesis doctoral, Universidad de Murcia.

DE GREGORIO (2011), «Niños y adolescentes en las redes sociales: una visión desde América Latina y el Caribe», en PIÑAR MAÑAS/RODOTÀ/OSORIO RODRÍGUEZ (coords.), *Redes sociales y privacidad del menor*, Editorial Reus, Madrid, pp. 263 ss.

HASSEMER (2010), «El Derecho penal en los tiempos de las modernas formas de criminalidad», en ALBRECHT/SIEBER/SIMON/SCHWARZ (coords.), *Criminalidad, evolución del Derecho penal y crítica al Derecho penal en la actualidad*, Editores del Puerto, Buenos Aires, pp. 15 ss.

HERRERA DE LAS HERAS (2014), «El derecho a la propia imagen de los menores de edad ante los medios de comunicación», *Diario La Ley*, (8319).

INTECO-AEPD (2012), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*.

MACÍAS CASTILLO (2008), «El consentimiento del menor y los actos de disposición sobre su derecho a la propia imagen», *Diario La Ley*, (6911 a 6913).

MARTÍNEZ OTERO/BOO GORDILLO (2012), «El fenómeno del *sexting* en la adolescencia: descripción, riesgos que comporta y respuestas jurídicas», en GARCÍA GONZÁLEZ (dir.), *La violencia de género en la adolescencia*, Aranzadi, Pamplona, pp. 291 ss.

MATALLÍN EVANGELIO (2015), «Delito de acoso (artículo 172 ter)», en GONZÁLEZ CUSSAC (dir.), *Comentarios a la reforma del Código penal de 2015*, Tirant lo Blanch, Valencia, pp. 575 ss.

MIRÓ LLINARES (2013), «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio», *Revista Española de Investigación Criminológica*, (11), pp. 5 ss.

———— (2012), *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Marcial Pons, Madrid – Barcelona – Buenos Aires – San Pablo.

——— (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*, (13).

MORALES PRATS (2015), «La reforma de los delitos contra la intimidad. Artículo 197 CP», en QUINTERO OLIVARES (coord.), *Comentario a la reforma penal de 2015*, Aranzadi, Pamplona, pp. 459 ss.

MORENO NAVARRETE (2010), «Aspectos jurídico privados de las tecnologías Web 2.0 y su repercusión en el derecho a la intimidad», en BOIX REIG (dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, pp. 335 ss.

MUÑOZ (2014), «El llamado 'derecho al olvido' y la responsabilidad de los buscadores. Comentario a la Sentencia del TJUE de 13 de mayo de 2014», *Diario La Ley*, (8317).

NIETO ALONSO (2008), «La relevancia del consentimiento del menor. Especial consideración a la anticoncepción en la adolescencia», *Diario La Ley*, (7041).

OROZCO PARDO (2010), «Intimidad, privacidad, 'extemidad' y protección de datos del menor ¿un cambio de paradigma?», en BOIX REIG (dir.), *La protección jurídica de la intimidad*, Iustel, Madrid, pp. 381 ss.

PICOTTI (2013), «Los derechos fundamentales en el uso y abuso de las redes sociales en Italia: aspectos penales», *Revista de Internet, Derecho y Política*, (16), pp. 76 ss.

PIÑAR MAÑAS (2011), «El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales», en EL MISMO (dir.), *Redes sociales y privacidad del menor*, Editorial Reus, Madrid, pp. 61 ss.

RODOTÀ (2011), «Sociedad contemporánea, privacidad del menor y redes sociales", en PIÑAR MAÑAS (dir.), *Redes sociales y privacidad del menor*, Editorial Reus, Madrid, pp. 35 ss.

RODRÍGUEZ LAINZ (2013), «Internet de los objetos y secreto de las comunicaciones», *Diario La Ley*, (8034).

——— (2013), «La interceptación de las comunicaciones telefónicas y telemáticas en el borrador de Anteproyecto de Código Procesal Penal», *Diario La Ley*, (8039).

——— (2011), «Los límites a la dimensión formal del derecho al secreto de las comunicaciones», *Diario La Ley*, (7669).

ROIG I BATALLA (2009), «E-privacidad y redes sociales», *Revista de Internet, Derecho y Política*, (9), pp. 42 ss.

——— (2006), «El anonimato y los límites a la libertad en internet», en COTINO HUESO (coord.), *Libertad en internet: la red y las libertades de expresión e información*, pp. 321 ss.

ROMEO CASABONA (2010), «Derecho penal y libertades de expresión y comunicación en Internet», en EL MISMO/SÁNCHEZ LÁZARO (eds.), *La adaptación del Derecho Penal al desarrollo social y tecnológico*, Comares, Granada, pp. 299 ss.

RUEDA MARTÍN (2013), «La relevancia penal del consentimiento del menor de edad en relación con los delitos contra la intimidad y la propia imagen. (Especial consideración a la disponibilidad de la propia imagen del menor de edad en el ciberespacio)», *Indret. Revista para el Análisis del Derecho*, (4).

TORRES ALBERO/ROBLES/DE MARCO (2014), *El ciberacoso como forma de ejercer la violencia de género en la juventud. Un riesgo en la sociedad de la información y del conocimiento*, Informe realizado para el Ministerio de Sanidad, Servicios Sociales e Igualdad, Centro de Publicaciones, Madrid.

TRONCOSO REIGADA (2012), «Las redes sociales a la luz de la propuesta de reglamento general de protección de datos personales», *Revista de Internet, Derecho y Política*, (15), pp. 61 ss.

VELASCO NÚÑEZ (2010), *Delitos cometidos a través de internet. Cuestiones procesales,* Editorial La Ley, Madrid.

VILLACAMPA ESTIARTE (2015), «El delito de stalking», en QUINTERO OLIVARES (coord.), *Comentario a la reforma penal de 2015*, pp. 379 ss.

ZOCO ZABALA (2010), «Interceptación de las comunicaciones electrónicas. Concordancias y discordancias de SITEL con el artículo 18.3 CE», *InDret. Revista para el Análisis del Derecho*, (4).

6. Tabla de jurisprudencia citada

Tribunal, Sala y Fecha	*Referencia*	*Magistrado Ponente*
STS, 4ª, 18.12.2014	–	Luis María Diez-Picazo Giménez
STS, 1ª, 26.11.2014	850/2014	Cándido Conde-Pumpido Tourón
STS, 1ª, 28.06.2013	575/2013	Manuel Marchena Gómez
STS, 1ª, 26.03.2013	165/2013	Joaquín Giménez García
STS, 1ª, 07.07.2011	663/2011	Diego Antonio Ramos Gancedo
SAN, 1ª, 26.09.2013	–	Eduardo Ortega Martín
AAP Madrid, 4ª, 25.02.2013	131/2015	José Joaquín Hervás Ortiz
SAP Asturias, 3ª, 07.03.2011	50/2011	Ana Mª Pilar Álvarez
SAP Jaén, 22.01.2009	10/2009	Mª Elena Arias-Salgado Robsy