REVISTA CHILENA DE DERECHO Y TECNOLOGÍA
CENTRO DE ESTUDIOS EN DERECHO INFORMÁTICO • UNIVERSIDAD DE CHILE
ISSN 0719-2584 • VOL. 5 NÚM. 1 (2016) • PÁGS. 63-94 • DOI 10.5354/0719-2584.2016.42557

La privacidad de los niños y adolescentes en las redes sociales: Referencia especial al régimen normativo europeo y español, con algunas consideraciones sobre el chileno

The Privacy of Children and Adolescents in Social Networks: Special Reference to the European and Spanish Regulatory Regime, with some Considerations on the Chilean

ÁNGEL ACEDO PENCO
Universidad de Extremadura, España

ALEJANDRO PLATERO ALCÓN
Universidad de Extremadura, España

RESUMEN Este artículo aborda la protección de datos personales de los niños y adolescentes en su relación con las redes sociales digitales. Se analizará, en primer lugar, a los niños como sujetos de derechos digitales, con especial atención al derecho fundamental de protección de datos, así como la validez de su consentimiento, no sólo para acceder a las redes sociales, sino también para la realización de actividades habituales como subir fotos y videos personales. En segundo lugar, se expondrán los principales peligros que las redes sociales esconden a los niños, para luego terminar con la exposición de algunas propuestas actuales para la protección de las personas que no han alcanzado la mayoría de edad.

PALABRAS CLAVE Redes sociales, tratamiento de datos, sexting.

ABSTRACT This paper addresses the protection of personal data of children and adolescents in their relationship to digital social networks. It will analyze, first, children as subjects digital rights, with special attention to the fundamental right to data protection, as well as the validity of consent, not only to access social networks, but also to perform usual activities as upload photos and personal videos. And secondly, the main dangers that social networks hide the children, finally, with exposure to some of the few proposals for the protection of persons who have not attained the age of majority are developing in will be exposed the present.

KEYWORDS Social networks, data processing, sexting.

INTRODUCCIÓN

En las siguientes páginas se analizan, desde diversos puntos de vista, algunos de los peligros, problemas y consecuencias derivados de la utilización de las redes sociales por quienes aún no han alcanzado la mayoría de edad, esto es, los niños y los adolescentes.

Por su grado de desarrollo, madurez y formación, los niños y adolescentes son especialmente sensibles a las percepciones externas y pese a ser sujetos de derecho, sus capacidades pueden estar afectadas en función de su edad y de sus vivencias, e incluso reducidas en la práctica para realizar con plena solvencia ciertos actos con relevancia jurídica, por la dificultad para comprender el significado y los efectos de sus acciones.

Hoy es muy común que los niños y jóvenes accedan a una o varias de las redes sociales más populares, sin embargo, no siempre serán conscientes de las consecuencias jurídicas que de ello se derivan. Así, raramente sabrán que están consintiendo el tratamiento automatizado de sus datos personales más íntimos, como sus imágenes, comentarios, ubicaciones, y otros tantos que luego quedarán almacenados en las bases de datos de la red social al alcance de muchas personas que pueden utilizar sus datos con fines lícitos o ilícitos, conductas que pueden ser calificadas de delito en los casos más graves.

Siendo universalmente aceptado el principio general del interés superior del niño, en todos los ámbitos jurídicos que le afectan (Ravetllat Ballesté y Pinochet Olave, 2015: 903-934), resulta decisivo conocer su grado de madurez para realizar ciertos actos, y entre éstos, el consenti-

miento, generalmente involuntario, o desconociendo sus efectos, para intervenir en las redes sociales y aportar sus datos más personales.

Lo anterior abre la posibilidad de invalidar el consentimiento del niño para el acceso a una red social sin el permiso de sus padres o tutores. La protección de la privacidad de los niños y jóvenes en internet está suscitando un enorme debate y, fruto de ello, gran cantidad de iniciativas internacionales pretenden aumentar el nivel de protección de estos derechos del niño.

LA RELACIÓN EXISTENTE ENTRE EL NIÑO Y LAS REDES SOCIALES

LAS REDES SOCIALES EN LA ERA DIGITAL

Aunque es difícil de precisar, se calcula que internet lo utilizan cotidianamente más de tres mil millones de personas, es decir, más del 40% de la población mundial. Las redes sociales son una de las herramientas más usadas por este canal de comunicación. Actualmente, son pocos los jóvenes en las sociedades desarrolladas que declaran no utilizar algunas de las más famosas, como Facebook, Instagram o Twitter.

Al margen de la acepción coloquial antes apuntada, las redes sociales se han definido, más técnicamente, como «servicios que se prestan a través de internet y que posibilitan a los usuarios crear un perfil púbico, donde plasman datos personales e información, contando con herramientas que permiten interactuar con el resto de usuarios, sean afines o no al perfil» (Inteco, 2009: 7).

Las redes sociales se han venido enmarcando dentro del concepto de web 2.0, que camina hacia

> una nueva tendencia en el uso de las páginas web, en la cual el usuario es el centro de la información y se convierte en generador de contenidos. Ello supone un cambio en la filosofía, una actitud, una forma de hacer las cosas que identifica el uso actual de internet que hacen tanto los internautas como las empresas, pasando de ser meros consumidores a productores y creadores de contenido (Heredero Campo, 2012: 40).

Esta etapa tecnológica es ya una evolución de otra etapa anterior, la web 1.0:

> En los medios tradicionales y en la denominada *web* 1.0 los dueños

> de los *websites* tienen pleno control sobre ellas, tanto de la información que exponen como del acceso y nivel de interactividad que quieren fomentar. Sin embargo, en la *web* 2.0 el control pasa directamente a todos los usuarios en igualdad de condiciones, el control está en los propios usuarios de la red social (Cebrian Herreros, 2008: 348).

Pero internet no deja de avanzar —es una de sus características— y, en la actualidad, la web 2.0 también se ha quedado obsoleta, destacando la denominada *web* 3.0, o *semantic web* (Martínez López, Anaya-Sánchez, Aguilar-Illescas y Molinillo, 2016: 5). Debe entenderse esta acepción de web semántica, como aquella que contiene un nivel de organización de ideas y contenidos que ofrece una respuesta rápida a la demanda de información necesitada individualmente.

Como se desprende de lo anterior, los avances digitales parecen imparables, pero:

> si bien el creciente desarrollo tecnológico representa grandes beneficios para las personas en términos de acceso al conocimiento y a la información, trae aparejado riesgos significativos para el titular de los datos personales, que circulan sin mayor control en la red, lo cual merma de manera importante la protección de su esfera privada y determinación informativa (Muñoz Massouh, 2015: 121).

La población vive actualmente con una demanda de información constante y con una necesidad, a veces incomprensible, de narrar sus acontecimientos vitales a través de las redes sociales, de tal suerte que se ha llegado a relacionar el ego con las redes sociales:

> el ego mueve el mundo y, sin duda, mueve las redes sociales, y en esta expresión continua de nuestro yo dejamos al descubierto su parte más íntima, sin ser conscientes, mientras lo hacemos, de cuánto de nosotros exponemos ni del peso que esa exposición tendrá en el futuro (Llaneza, 2010: 57).

En nuestra opinión, el uso de internet ha puesto de moda, universalizándolos, una serie de derechos como la libertad de información y la libertad de expresión, pero, al mismo tiempo, ha generado graves riesgos para la indemnidad de otros derechos fundamentales, no menos importantes, como el de protección de datos personales, el derecho a la intimidad, es decir, aquellos que afectan al círculo de la privacidad de las personas.

Las redes sociales, como casi todos los fenómenos de gran relevancia de los grupos humanos, se comportan como armas de doble filo, ya que, por una parte, su funcionamiento intrínseco permite al ciudadano que usa medios electrónicos comunicarse con personas que estén en cualquier lugar del mundo (a unos metros o al otro lado de la Tierra), o permiten observar las fotos o videos que sus «amigos» deciden compartir, imágenes que, en ocasiones, se suben sin meditarlo mucho.

¿Qué ocurre si alguien decide utilizar esas fotografías para publicarlas con alguna información que puede ser dañina, o si decide utilizar los comentarios vertidos en redes sociales con el mismo fin? La respuesta puede llegar a ser inquietante ya que el daño producido, o que se pueda generar en un futuro incierto, quizá sea irreversible: esas imágenes, información vertida y datos íntimos que una persona ha querido divulgar a través de estas redes sociales pueden perjudicarle en el futuro (Platero Alcón, 2016).

Como ejemplo, en los procesos de selección de personal estadounidenses, más del 35% de las empresas no contrataron a determinados trabajadores debido a las informaciones que habían descubierto investigando su pasado en las redes sociales (Adsuar Prieto, 2013: 6). Es conocido el caso de la ejecutiva de la industria del cine Stacy Snyder,[1] graduada en Leyes, quien no fue contratada como profesora por la Conestoga Valley High School por difundir una imagen suya tomando una bebida alcohólica.

Aunque la mayoría de los usuarios lo desconocen, las empresas que gestionan las redes sociales están continuamente realizando la actividad jurídica de tratamiento automatizado de los datos personales de quienes difunden datos de su vida privada y de sus preferencias.

RECONOCIMIENTO NORMATIVO

En algunos tratados internacionales universales

La protección de la privacidad está reconocida, con carácter general, en el artículo 12 de la Declaración Universal de los Derechos Humanos, al

1. Caso *Drunken Pirate*, MTV News, 2008, disponible en http://www.mtv.com/news/1558467/woman-denied-degree-over-drunken-pirate-myspace-photo-sues-school/. El asunto llegó a la Corte de Pennsylvania que falló a favor de la Escuela de Lancaster que le negó el título de profesora por tal difusión en *Myspace.com*; se encuentra disponible (en inglés) la sentencia citada en https://goo.gl/mUk4kn.

señalar: «Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

Dos décadas después, se firmó en Nueva York el Pacto de Derechos Civiles y Políticos, cuyo artículo 17 determina: «Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. [...] Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».[2]

Ya con carácter específico para los sujetos objeto de nuestro análisis, se reconoce el derecho a la protección de la vida privada en el artículo 16 de Convención sobre los Derechos del Niño, adoptada por la Asamblea General de las Naciones Unidas el 20 de noviembre de 1989.

En el ámbito de la Unión Europea

En el área comunitaria europea, que la integran 28 países en la actualidad,[3] el derecho a la protección de datos se ha reconocido como un derecho fundamental del individuo en la Carta de los Derechos Fundamentales de la Unión Europea de 18 de diciembre de 2000, cuyo artículo 8 determina:

> toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

2. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966 y que entró en vigor el día 23 de marzo de 1976.

3. Alemania, Austria, Bélgica, Bulgaria, Chipre, República Checa, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal y Reino Unido, aunque este último país ha iniciado un proceso de desconexión jurídica tras el resultado del referéndum sobre el *Brexit* celebrado el 23 de junio de 2016.

Su desarrollo consta en la Directiva 95/46/CE de 24 de octubre de 1995, del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Según su artículo 1, su objeto es «la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».[4]

No se podían prever los avances que la revolución digital iba a producir en el mundo (Batuecas Caletrío, 2015), por lo que la Comisión Europea aprobó el 25 de enero de 2012 una 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 datos, propuesta que ha sido modificada en numeras ocasiones, y cuyo último texto disponible se encuentra en el mes de junio del año 2015.[5]

Aunque el Reglamento entró en vigor en 2016, no será plenamente aplicable hasta la primavera de 2018, por lo tanto mientras tanto seguirá vigente la normativa anterior.[6]

RECONOCIMIENTO EN ESPAÑA

El estudio del caso de España resulta aquí especialmente interesante porque contiene el régimen jurídico sobre la materia en la Unión Europea, y por cuestiones de idioma, resulta más fácil su comparación con los sistemas de América Latina.

El derecho fundamental a la protección de datos se consagrada en el artículo 18.4 de la Constitución Española, según el cual, «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

La regulación instrumental del derecho fundamental a la protección

4. Artículo 1 de la Directiva 95/46/CE (24/10/1995) del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

5. Disponible en http://data.consilium.europa.eu/doc/document/st-9565-2015-init/es/pdf.

6. Documento disponible en http://www.consilium.europa.eu/es/policies/data-protection-reform/data-protection-regulation.

de datos se encuentra en el ordenamiento jurídico Español en la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos (LOPD) y su Reglamento aprobado por el Real Decreto 1720/2007, de 19 de enero. En su primer artículo, la Ley establece que el objeto de la ley es «garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar».[7]

EL CONTEXTO AMERICANO Y ALGUNA MENCIÓN A CHILE

La Convención Americana sobre Derechos Humanos o Pacto de San José de Costa Rica[8] establece en su artículo 11 sobre Protección de la Honra y de la Dignidad:

> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

En particular, su artículo sobre Derechos del Niño determina que: «Todo niño tiene derecho a las medidas de protección que su condición de niño requieren por parte de su familia, de la sociedad y del Estado».

La Constitución chilena no contiene una norma expresa en relación a la protección de datos personales, sin embargo, sigue en buena parte el modelo del artículo 12 de la Declaración Universal de Derechos Humanos, por lo que dicha protección constitucional se puede derivar de lo establecido en el artículo 19 número 4 que establece que la Constitución asegura el respeto y protección a la vida privada y a la honra de la persona y de su familia.

La Corte Suprema chilena se ha servido de dicho precepto para condenar casos donde se suben a internet fotos de terceras personas unidos

7. Artículo 1 de Ley Orgánica 15/1999 (13/12/1999) de protección de datos de carácter personal.

8. Esta Convención se adoptó tras la Conferencia Especializada Interamericana de Derechos Humanos, el 22 de noviembre de 1969 en San José en Costa Rica, entrando en vigor el día el 18 de julio de 1978.

a posibles comentarios denigrantes, siendo éste uno de los contenidos esenciales del derecho a la protección de datos (Figueroa García, 2013: 875). Chile fue el primer país de Latinoamérica que promulgó una ley de protección a la privacidad, la Ley 19.628[9] sobre Protección de la Vida Privada, del 18 de agosto de 1999, que contiene los principios fundamentales de la protección de datos personales en este país andino (Chen Mok, 2010: 128).

LA ATRACCIÓN DE NIÑOS Y JÓVENES A LAS REDES SOCIALES

Aunque muchas veces nos cueste asimilarlo, son muchos los niños que a partir de los doce años empiezan a darse a conocer en las redes sociales. Naturalmente, ello se debe al llamado *boom* digital, que trajo consigo a los *nativos digitales* (Bauerlein, 2008: 43), es decir, aquellos niños que han ido creciendo con un uso de internet ya consolidado, y en buena medida dependientes de las nuevas tecnologías, que puede llegar a ser una adicción.

Pero es bien sabido que los niños y jóvenes también son sujetos de derecho, con plena capacidad jurídica, y que también ostentan una serie de facultades y derechos, entre los que se encuentra, en un lugar destacado, el respeto a su intimidad e imagen personal, lo que implica necesariamente ciertas limitaciones de uso de las redes sociales para salvaguardar el contenido del derecho fundamental a la protección de datos.

En síntesis, la actuación de una red social, consistente en tener disponible la información publicada y colgada por terceros, para que otras personas, normalmente sus amigos *online*, puedan interactuar con la misma. Sin embargo, los niños no saben que acceder a las redes sociales puede suponerles graves perjuicios derivados de la posibilidad de que otras personas accedan a su intimidad personal y darle un uso indeseable, no querido por el niño, ahora o en el futuro.

Los riesgos de las redes sociales no suelen ser percibidos por los jó-

9. La Ley 19.628 en artículo 2 letra g) define los *datos sensibles*, como «aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual».

venes —ni muchas veces por los mayores de edad—, que se encuentran sumergidos en lo que algún autor denomina «la cultura de la habitación» (Gil Antón, 2013: 72), un mundo interior que desarrollan en sus estrictos ámbitos solitarios, donde se enfrascan en la vida *online* que les proporciona sus tabletas, ordenadores, teléfonos móviles inteligentes o aparatos de videojuegos.

Nadie duda de que la sociedad se ha transformado en poco tiempo debido a la revolución digital convirtiendo a los niños y adolescentes —aunque no solo a ellos— «en verdaderos agentes de penetración y alfabetización tecnológica en los hogares» (Marco Marco, 2010). Esta mutación ha provocado otro fenómeno conocido como el *networked individualism*, o individualismo en red, caracterizado por el abandono de los espacios públicos por parte de la población, replegándose a la intimidad del hogar, para poder vivir su vida en línea (Wellman y otros, 2003: 5). Otros autores establecen acertadamente que mientras los adultos viven con internet, los jóvenes viven en internet, hasta el punto de que las redes sociales son una parte indispensable de su vida (Piñar Mañas, 2011: 62).

La sociedad ha cambiado, transformando fundamentalmente a los niños, convirtiéndoles, a veces, en verdaderos adictos al uso de las nuevas tecnologías, lo que puede provocar, casi siempre, agresiones a la privacidad.

No creemos que haya que eliminar las posibilidades de acceso de los niños y jóvenes a las redes sociales, pues su uso adecuado puede generar beneficios, por ejemplo utilizándolas para contactar con amigos o familiares, compartir información útil, y cómo no, como herramientas de conocimiento o aprendizaje, a través, de la creación de redes sociales verticales.[10] Las redes sociales tienen ciertas ventajas de su uso, pero también contienen graves amenazas potenciales que pueden perjudicar el ámbito de privacidad del individuo.

En esta línea, se ha indicado con solvencia que

> las redes sociales *online* son el mejor ejemplo de la sociedad representada en un entorno creado tecnológicamente: ilustran tanto los beneficios sociales de comunicación y conexión entre individuos como

10. Sobre las redes sociales verticales, véase Gómez García, Ruíz Palmero y Sánchez Rodríguez (2015). Véase también Vanderhoven, Schellens y Valcke (2014).

> suscitan problemas de privacidad y falta de confianza en la veracidad de las informaciones (Díaz Cortés, 2010: 174).

Naturalmente, y así se ha avanzado más arriba, los principales peligros que entrañan las redes sociales se relacionan con posibles violaciones de ciertos derechos fundamentales: el derecho a la intimidad personal y familiar, el derecho a la propia imagen, y el derecho fundamental a la protección de datos, e incluso el derecho al honor, cuyo ámbito es mucho más amplio.

Estas violaciones son de mayor gravedad si se producen sobre los derechos de los niños y jóvenes, sujetos frágiles que desconocen las consecuencias de divulgar sus fotos, ideas, o sus datos personales más íntimos, en una red social ya que, «carecen de la madurez suficiente que requiere comprender las consecuencias que tienen ciertas acciones realizadas en ellas» (Batuecas Caletrío, 2015: 150).

En España, los derechos al honor, a la intimidad personal y familiar y a la propia imagen se consagran en el artículo 18.1 de la Constitución, donde se establece que «se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen».[11] Estos derechos fueron desarrollados por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Esta Ley establece una serie tipificada de intromisiones ilegítimas en los derechos al honor, la intimidad y la propia imagen, siempre y cuando no medie el consentimiento del afectado, o cuando tal consentimiento carezca de validez.[12]

En el caso de las redes sociales, este consentimiento es otorgado —sin saberlo— por los niños y jóvenes que acceden a las mismas desde el mismo momento en que aceptan sus políticas de privacidad. Por eso, la madurez de los niños a tales efectos es objeto de amplio debate, ya que, tal acceso puede acarrear graves consecuencias que raramente se llegan a prever.

Desde hace tiempo se debate acerca de la autonomía del derecho a la propia imagen[13] respecto al derecho a la intimidad personal, sosteniendo

11. Artículo 18.1 de la Constitución española.

12. Un estudio sobre el derecho al honor, la intimidad personal y familiar, y la propia imagen, donde citamos una amplia bibliografía, puede verse en nuestra obra, Acedo Penco (2007).

13. Véase Lathorp (2013).

la mayor parte de la doctrina que «la propia imagen en privado es inequívocamente parte del derecho a la intimidad, pero la propia imagen en público parece que no será parte del derecho a la intimidad» (Ruíz Miguel, 1995: 44). Sin embargo, en el caso de la actuación de los niños y jóvenes en las redes sociales, al margen de ello, conviene ahora aproximarse a un término que englobe ambas magnitudes, pareciendo el más adecuado el que se denomina *identidad digital*.

Puede entenderse por identidad digital «el conjunto de rasgos que nos caracterizan frente a los demás. El término 'identidad digital' pone el énfasis en aquellos rasgos del individuo que encontramos digitalizados y que están a disposición de los demás». Y se añade que «el uso generalizado de Internet, las prestaciones de los nuevos terminales móviles, la cada vez mayor participación de los ciudadanos en las redes sociales, junto con potentes herramientas de proceso de toda esta información, hacen posible que cada vez haya más datos de cada uno de nosotros a disposición de los demás» (Pérez Subía, 2012).[14]

En efecto, aplicado el concepto a los niños, jóvenes y adolescentes, la identidad digital debe ser el bien jurídico protegido ante la interacción de éstos en las redes sociales, identidad digital que hande tener presente que se configura como una potestad de quien no tiene la mayoría de edad de dar a conocer aspectos personales e íntimos, a veces difundiendo fotos o videos, o a través de comentarios.

Tal es la reflexión de algunos autores que, conscientes del diferente pensamiento que ostentan los nativos digitales, señalan que «el colectivo de jóvenes y adolescentes, que ha nacido con la tecnología plenamente arraigada, tiene una concepción diferente, tanto de los aspecto de la propia vida íntima, como de la propia figura» (Gil Antón, 2015: 75).

La preocupación por la privacidad de los niños y jóvenes en las re-

14. Véase Pérez Subías (2012), en cuyo trabajo su autor llega a las siguientes conclusiones al respecto: «Desarrollar estrategias en lo personal y en el ámbito educativo que nos permitan conocer y gestionar de forma efectiva nuestra identidad digital por su impacto en nuestra vida personal, social y profesional. Implementar ecosistemas globales de identificación formal que sean seguros y reconocidos por todos los países, que le permitan al usuario ser uno mismo, autenticarse siempre que se requiera de una forma segura y sencilla. Crear una regulación que aporte transparencia, dándole al usuario el conocimiento y la capacidad de decidir sobre la información personal que recogen de él las aplicaciones y sobre los potenciales usos que puedan hacerse de ella».

des sociales ha propiciado la aparición de recientes estudios sociológicos que tratan de averiguar la dimensión social de este fenómeno mediante la medición de dos variables relacionadas, el número de niños que las utilizan y sus niveles de conocimiento sobre ellas.

Destaca el de la Universidad Internacional de la Rioja de julio de 2013, sobre el uso de internet y las redes sociales de los adolescentes españoles de 12 a 18 años, donde se indica, entre otras muchas conclusiones, que el 21,2% de los adolescentes españoles ha recibido alguna petición de foto comprometedora, y que más del 50% consideran que lo que escriben o suben a las redes sociales les puede ocasionar problemas en el futuro (Ibáñez Martín, 2013: 32).

Otras investigaciones reflejan resultados positivos sobre la intención de los jóvenes de aumentar las precauciones en su actuación en las redes sociales, como el estudio publicado en junio de 2014, que analiza a los jóvenes de 14 a 20 años españoles y llega a la conclusión de que tan sólo un 18,4% de los jóvenes analizados declaran relacionarse con desconocidos en las redes sociales donde participan activamente (Sabater Fernández, 2014: 21).

Han sido analizados los datos sobre el uso de las redes sociales por niños y jóvenes en Colombia y España, aportando las diferencias existentes entre los usuarios niños colombianos y españoles, de 12 a 15 años en sus actuaciones en Facebook, resultando que, de una muestra de 100 niños y jóvenes de ambos países, la mayoría participa en esta red social, destacando, como dato curioso diferencial, que mientras los niños españoles utilizan su nombre real en más de un 90% de los casos, en Colombia, este porcentaje se rebaja al 55% (Almansa, Fonseca y Castillo, 2013: 130).

LA COMPLEJIDAD DE LOS DERECHOS DE LOS NATIVOS DIGITALES

¿ES VÁLIDO EL CONSENTIMIENTO PRESTADO POR EL NIÑO?

En la práctica, para acceder a una determinada red social, cualquier usuario debe registrarse mediante un proceso donde el prestador del servicio exige que se manifieste el consentimiento sobre las condiciones de privacidad del mismo (términos de uso). Se pide al potencial usuario de la red social que realice una lectura de los términos de uso, y una vez afirme que los ha comprendido, preste o no el consentimiento.

Pero no parece razonable entender que el niño y el joven —ni, en muchas ocasiones, los mayores de edad— tengan todos los elementos de juicio necesarios para comprender los peligros que le puede reportar compartir sus opiniones, comentarios, datos o imágenes personales en las redes sociales. Y aún en el caso de que los comprenda, el régimen jurídico existente para que el niño preste su consentimiento, se encuentra lleno de dudas jurídicas que podrían afectar a la validez del mismo.

Como es sabido, el consentimiento es uno de los elementos esenciales de cualquier contrato, figura regulada por el derecho civil de todos los ordenamientos jurídicos del mundo. El vigente Código Civil de Chile lo exige preceptivamente en su artículo 1445 para que una persona pueda obligarse eficazmente y el ordinal siguiente establece una presunción general de capacidad limitándola sólo a quienes la ley determine: «Toda persona es legalmente capaz, excepto aquellas que la ley declara incapaces», entre las que se encuentran los «impúberes» y los «menores adultos» en el artículo 1447.

Sin embargo, el párrafo segundo de este último precepto amplía considerablemente la restricción inicial y determina que la incapacidad legal de ciertas personas: «no es absoluta, y sus actos pueden tener valor en ciertas circunstancias y bajo ciertos respectos, determinados por las leyes».

En línea muy similar, en España, el consentimiento contractual, regulado en los artículos 1261 a 1270 del Código Civil español,[15] establece en el 1263 que no podrán prestar consentimiento los menores no emancipados, ni los incapacitados por sentencia judicial. Parecería, en sentido literal, que la regla general en el ordenamiento jurídico español es que el niño no podrá prestar el consentimiento para obligarse. Sin embargo, la rotundidad del citado precepto ha decaído considerablemente con la entrada en vigor del artículo 2 de la Ley Orgánica 1/1996 (17/01/1996) de Protección Jurídica del Menor, al determinar que «las limitaciones a la capacidad de obrar de los menores se interpretarán de forma restrictiva y, en todo caso, siempre en el interés superior del niño» (Acedo Penco, 2013: 77).

15. Artículo 1261 del Real Decreto 206 de 24 de julio de 1889: No hay contrato sino cuando concurren los requisitos siguientes: 1) consentimiento de los contratantes, 2) objeto cierto que sea materia del contrato, 3) causa de la obligación que se establezca.

Además, como se indicó anteriormente, el niño es titular de un derecho al honor, a la intimidad y a su propia imagen, unos derechos que les son propios por ser persona, de suerte tal que «tanto la capacidad jurídica como la capacidad de obrar son manifestaciones directas de la personalidad, la primera de forma pura y directa, la segunda de forma gradual en función del autogobierno existente» (Gordillo Cañas, 1986: 57). Por ello, actualmente se viene elevando, de facto, el número de actuaciones que pueden realizar los niños y jóvenes por sí mismos, como contraer matrimonio, o adoptar un testamento válido.

Normalmente, como fundamento de estas actuaciones, suele aparecer la alusión a la madurez del menor. La madurez del menor justifica que el niño pueda otorgar su consentimiento para realizar cualquier acto acorde con su madurez, como sería acceder a una determinada red social, en virtud de lo establecido en el artículo 162 del Código Civil español, que determina que se exceptúa de la patria potestad de los padres «los actos relativos a los derechos de la personalidad que el hijo, de acuerdo con su madurez, pueda ejercitar por sí mismo. No obstante, los responsables parentales intervendrán en estos casos en virtud de sus deberes de cuidado y asistencia».

Ahora bien, ¿es posible hacer depender la validez del consentimiento del niño para acceder a una red social, simplemente de su grado de madurez? La respuesta a ésta cuestión es compleja, ya que podría convertirse en una *probatio diabolica* la exigencia, para poder registrarse en ella, de la comprobación de la capacidad de los niños y jóvenes, individualmente considerados. Parece aconsejable, por ello, añadir otro criterio, mucho más objetivo, que a través de una interpretación conjunta con la madurez permita al niño prestar un consentimiento válido, como es la edad del menor.

Así, el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos en España establece, en su artículo 13, que «podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los niños y jóvenes de catorce años se requerirá el consentimiento de los padres o tutores».[16]

16. Real Decreto 1720/2007 (19/01/2008) por el que se aprueba el Reglamento de

En función de lo anterior, en el ordenamiento jurídico español, los niños y jóvenes que tengan catorce años o más podrán consentir válidamente para acceder a una red social, mientras que los niños menores de trece años, deberán recabar el consentimiento de sus padres.

Existen numerosas críticas a este precepto. En primer lugar, por la técnica legislativa utilizada, ya que, al tratarse de un derecho fundamental, esta cuestión no debería contenerse en un reglamento, debiendo ser declarado inconstitucional;[17] y, en segundo lugar, por la falta de consonancia entre fijar una edad para consentir válidamente actos jurídicos y la necesidad de madurez del menor que el artículo 162.1 del Código Civil establece.

Tal vez el artículo 162.1 debería interpretarse en el sentido de establecer una presunción general de que el joven o adolescente menor de 18 años pero con 14 o más, ostenta una madurez suficiente como para poder prestar un consentimiento válido para acceder a las redes sociales. Así lo consideran ciertos autores, indicando que una especie de presunción *iuris tantum* de madurez a favor del mayor de 14 años, lo que implica que a los mayores de dicha edad se les presupone madurez suficiente para prestar el consentimiento para el tratamiento de sus datos personales (Batuecas Caletrio, 2015). Pero otros autores consideran que el señalamiento de esta edad de 14 años, es un acto arbitrario y falto de explicación, ya que igualmente se podría haber fijado cualquier otra (Andreu Martínez, 2013: 75).

Sin embargo, el criterio de la edad es el más objetivo, sencillo e igualitario y resuelve un problema que de otra manera parece difícil o imposible solventar. Además, no sería admisible pensar en un ordenamiento que permitiera a un adolescente de 14 años realizar un acto de tanta importancia, como es la otorgación de un testamento,[18] y, sin embargo, no le permitiera acceder a una red social, de suerte tal que «no podemos caer en un exceso de paternalismo que suprima la autonomía de los

Desarrollo de la Ley Orgánica 15/1999 (13/12/1999) de Protección de Datos de Carácter Personal.

17. Véase Plaza Penadés (2008). Véase Vázquez de Castro (2012).

18. Artículos 662 y 663 del Código Civil español y artículo 1005.2, en relación con el artículo 26 del Código Civil de Chile. Ambos textos legales permiten otorgar testamento al mayor de catorce años de edad.

menores, algo necesario para el desarrollo de su personalidad, aunque parece razonable exigir a las redes sociales a restringir al máximo grado de privacidad el acceso a los perfiles de los menores, y limitar el número de amigos» (Troncoso Reigada, 2012: 73).

Los problemas sobre la validez del consentimiento prestado por el niño para acceder a una red social no se agotan con su registro y acceso, sino que se incrementan cuando aquél divulga comentarios, datos e imágenes personales. En tal caso pueden operar también otros instrumentos legales cuando, por ejemplo, se produzca una intromisión en el derecho al honor, a la intimidad y a la propia imagen del menor (Grimalt Servera, 2013).

Así, en España, la primera norma que deber ser tenida en cuenta es la citada Ley de Protección al Derecho al Honor, Intimidad y a la Propia Imagen, en cuyo artículo 3.1 determina que «el consentimiento de los menores e incapaces deberá prestarse por ellos mismos si sus condiciones de madurez lo permiten, de acuerdo con la legislación civil».

Igualmente, opera respecto al sistema de validez del consentimiento del niño la Ley Orgánica 1/1996, de 17 de enero de 1996, de Protección Jurídica del Menor, cuyo artículo 4.3 establece:

> Se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales.

Este precepto complica aún más la cuestión, ya que introduce la posibilidad de que un menor, con 14 años o más, que cuente con madurez suficiente, puede que carezca de la autorización legal precisa para confirmar un determinado tratamiento de datos debido a que puede ser contrario a sus propios intereses. La doctrina critica esta posición legal, debido a su más que probable inaplicación en caso de redes sociales. Parece más lógico extender su aplicación incluyéndolas dentro de la mención legal expresa referida a los «medios de comunicación» (Martínez Martínez, 2013).

En los casos de intromisión al honor o lesión a la imagen del menor, esta última Ley faculta al Ministerio Fiscal a actuar de oficio para proteger el interés del menor, lo que ha sido objeto de críticas diciéndose que

«no somos partidarios del reforzamiento que se pretende, ni de la forma en la que se lleva a cabo, en la medida que choca frontalmente con el principio de capacidad del menor» (Rovira Suero, 2000: 127).

Sin embargo, esta actuación de oficio debe justificarse en aras de proteger el interés del menor, como se añade desde otra óptica al considerar que «aunque el menor con madurez suficiente puede consentir válidamente por sí mismo la intromisión en su derecho a la imagen, cuando dicha intromisión sea contraria a su personalidad o a su derechos fundamentales deberá intervenir el Ministerio Fiscal a posteriori para proteger el interés del menor» (De Lama Ayma, 2006: 170).

En vista de lo anterior, el sistema actual deja en manos de los tribunales la decisión última acerca de la validez de la actuación del niño en las redes sociales aunque éste supere los 14 años, ya que, aun así, divulgar sus imágenes o mantener determinadas conversaciones con adultos mayores de edad, puede suponer una violación de sus derechos fundamentales al honor, a la intimidad y a la propia imagen.

Quizás, fruto de tan insegura situación jurídica, en determinadas ocasiones la actuación del menor será inválida y no será difícil que sea declarada lícita, por lo que el legislador comunitario europeo lleva desde el año 2012 intentando mejorar el sistema de acceso del menor a las redes sociales. La propuesta de Reglamento Europeo de protección de datos, que se espera que entre en vigor en el año 2018, introduce un nuevo sistema al descrito anteriormente. Su artículo 8 introduce la edad de 13 años a partir de la cual será válido el consentimiento para acceder a las redes sociales. Cuando un menor de dicha edad acceda a las redes sociales sin consentimiento expreso de sus tutores legales, el responsable de dicha actuación será la propia red social, que deberá tener habilitados mecanismos para evitar tales conductas.

A veces se utilizan perfiles de control de la actividad que se produce en la misma, o se instala algún software específico que detecta la edad del usuario mediante la identificación de su leguaje o fotos (Inteco, 2009: 19). Parte de este software se basa en la idea del modelo de madurez donde se detallan los diferentes ámbitos de protección de las redes sociales y se describen cinco niveles de madurez (inicial, repetible, definido, gestionado y optimizado) y cada uno de ellos se divide, a su vez, en diferentes procesos y subprocesos de gestión (Coz Fernández y otros, 2012: 69).

Como se adelantó, el consentimiento del niño para acceder a una red social puede verse condicionado legalmente por la consideración del contrato que se produce con la misma como oneroso o gratuito. Es indudable, aunque el niño no lo perciba en el desarrollo de su actividad de comunicación en la red social, que ésta, junto a los motores de búsqueda en internet, se dedican a tratar sus datos personales, a comercializarlos, obteniendo por ello una enorme rentabilidad.

En este sentido, destacan numerosos estudios que intentan dar luz al oscuro negocio del tratamiento de datos personales, como el realizado por Tucker, que ya en el año 2009 llegó a la conclusión de que el negocio publicitario obtenido a través de los datos personales de los estadounidenses ascendía a 22.000 millones de dólares.[19]

Ahora bien, desde el año 2009 esta rentabilidad no ha dejado de crecer, como demuestra el último informe sobre la industria publicado por el IAB en Estados Unidos, donde se desprende que en el año 2014 el rendimiento alcanzó 49.500 millones de dólares, y que en el primer semestre del año 2015, ya se había superado la cantidad de 27.500 millones de dólares.[20] A nivel Europeo, los datos tampoco parecen desinflarse, ya que la Comisión Europea estima que para el año 2020, los datos de los ciudadanos europeos alcanzarán una rentabilidad económica cercana al billón de euros.[21]

Algunas investigaciones, han profundizado en este negocio, llegando a identificar diferentes tipos de mercados donde comercializar los datos privados.[22] No sólo del negocio publicitario viven las redes sociales, ya

19. Vease E. Tucker, «The economic value of online customer data», *The economics of Personal Data and Privacy. 30 Years afther the OECD Privacy Guidelines*. Disponible en http://www.oecd.org/sti/ieconomy/theeconomicsofpersonaldataandprivacy30yearsaftertheoecdprivacyguidelines.htm.

20. Véase el *IAB Internet Advertising Revenue Report, 2015 first six months result*s, disponible en http://www.iab.com/wpcontent/uploads/2015/10/IAB_internet_Advertising_Revenue_Report_HY_2015.pdf.

21. *European Commision- Fact Sheet* MEMO/15/5170/, de 15 de junio de 2015.

22. Véase Acquisti, Taylor y Wagman (2015). Estos autores consideran que existen tres tipos de mercados donde los comercializar los datos privados: Mercados ordinarios de bienes y servicios, Mercados de datos personales, y Mercados de productos o servicios para gestionar la protección de datos personales.

que las preferencias del usuario otorgan una información de mayor utilidad para los prestadores de servicios, pudiendo rediseñar sus productos o servicios en función de las preferencias de los usuarios, gustos que en ocasiones pueden variar incluso por regiones geográficas.

Este tratamiento con fines de predicción también puede producir otras ventajas. Así, «son muchos los ámbitos en los que del uso de los datos pueden derivarse beneficios, por ejemplo en el tratamiento de las enfermedades, el control de epidemias, o la protección frente al fraude, entre otros» (Hernández Martín, 2015).

Resulta impreciso determinar el grado de conocimiento que puede albergar un niño, en relación al rentable negocio descrito anteriormente, más aun, cuando todavía existe otra vertiente que no ha sido descrita. En efecto, el negocio del tratamiento de datos personales puede todavía complicarse un poco más, destacando algunos recientes estudios que muestran cuál es el valor monetario de un dato personal concreto incluido en las redes sociales, como la edad, el sexo o la ubicación.

Así, por ejemplo, datos como los enunciados anteriormente se pueden adquirir a 50 céntimos de dólar por cada mil individuos.[23] En vista de lo anterior, parece que los datos personales por cada individuo tienen un escaso valor, pero el negocio se encuentra en la atracción de grandes cantidades de personas, de suerte tal que si se multiplica los 1.500 millones de usuarios de Facebook por la cantidad anterior, el negocio puede ser extraordinario.

La Universidad de Twente ha publicado recientemente una investigación relacionada con el conocimiento que tienen los usuarios pasivos de un tratamiento de datos personales, obteniendo como resultado reseñable que un 47% de los usuarios estarían dispuestos a publicar más datos personales a cambio de un pago monetario por parte del responsable del tratamiento de datos.[24] Este dato es preocupante, más aún si se piensa en los niños y jóvenes, personas con menores recursos económicos que los adultos, y que podrían ser grandes víctimas de servicios de este tipo.

23. Vease Steel, Locke, Cadman y Freese (2013).

24. Vease Karlijn (2015).

LA CRECIENTE PREOCUPACIÓN POR LA PRIVACIDAD DEL MENOR

LOS PELIGROS DE LAS REDES SOCIALES PARA EL MENOR

Hasta ahora hemos puesto de manifiesto las dudas sobre el grado de conocimiento de los niños y jóvenes acerca de los derechos que les amparan en el ejercicio de esta nueva forma de comunicación, y su grado de conocimiento sobre el funcionamiento y actividad de los prestadores de servicios *online*. Pero es el momento de hacer mención a los peligros específicos en que se traducen las posibles violaciones de los derechos de los niños en internet.

El ciberacoso es una conducta a través de la cual se produce un acoso a otra persona, una agresión psicológica, transmitiendo información difamatoria hacia otra persona mediante los medios tecnológicos.

Una variante muy importante del ciberacoso, en cuanto a sus efectos negativos, es el denominado *ciberbullying*, el cual supone «el uso y difusión de información lesiva o difamatoria en formato electrónico a través de medios de comunicación como el correo electrónico, la mensajería de texto a través de teléfonos o dispositivos móviles o la publicación de videos y fotografías en plataformas electrónicas de difusión de contenidos» (Marco Marco, 2010: 90).

La característica fundamental de esta variante del ciberacoso reside en sus sujetos intervinientes, ya que tanto el sujeto activo como el sujeto pasivo no alcanzan la mayoría de edad legal. El *ciberbullying* destaca por el anonimato del agresor, ya que suele actuar en redes sociales a través de nombres falsos, y por la vulnerabilidad de la víctima, que al tratarse de un niño, probablemente con menor grado de madurez que su agresor también menor, suele revelar gran cantidad de información personal (Berrocal Lanzarot, 2013: 18).

El ordenamiento jurídico español sanciona esta conducta con una pena de prisión que oscila entre los seis meses y los dos años de prisión.[25] Independientemente de la posible responsabilidad en vía penal, también podrá solicitarse en vía civil, ya que la Sentencia del Tribunal Constitucional español número 241/1991, de 16 de diciembre, en su fundamento

25. Artículo 173 del Código Penal español, aprobado por la Ley Orgánica 10/1995, de 23 de noviembre.

jurídico cuarto, estableció que «cuando tengan ocasión intromisiones ilegítimas en los derechos de la personalidad a través de los medios de comunicación, existe la posibilidad de acudir ante la Jurisdicción civil o la penal, indistintamente».

Además, aún en el caso de que un determinado país de la Unión Europea no tenga una regulación exacta de este tipo de acoso, debe entenderse que este derecho se encuentra protegido por el artículo 8 de la Carta de Derechos fundamentales de la Unión Europea. Así lo estableció el Tribunal de Justicia de la Unión Europea, en un caso donde se enjuiciaba un anuncio en un portal de citas en Finlandia, colocado por un desconocido, donde se podría observar el nombre de un niño de 12 años de edad, sin su conocimiento. El anuncio incluía la edad del niño, una descripción de sus características físicas, un enlace a su página web que contenía una imagen y un número de teléfono, y una declaración de que el desconocido que puso el anuncio estaba buscando una relación íntima con un niño.

En el momento de los hechos no era posible, de acuerdo con la normativa finlandesa, la obtención de la identidad de la persona que colocó el anuncio en el proveedor de internet, pero la Corte consideró indiscutible la aplicabilidad del artículo 8 del Convenio Europeo de Derechos Humanos y destacó que los niños y otras personas vulnerables tienen derecho a la protección del Estado, en la forma de disuasión efectiva, a partir de tales interferencias en los aspectos esenciales de su vida privada (Lievens, 2014: 258).

El *sexting* es una conducta que puede ser definida como el envío de mensajes de contenido sexual y de forma voluntaria por parte de una persona a otra, cuando entre ellos existe una relación de confianza. Otros autores consideran esta figura más amplia, incluyendo incluso los mensajes de textos, definiendo el *sexting* como «la escritura entre jóvenes de mensajes sexualmente explícitos, tomando fotos sexualmente explícitas de sí mismos u otros en su grupo de pares, y [la transmisión de] esas fotos y/o mensajes a sus compañeros» (Sacco y otros, 2010: 3).

Entre los más jóvenes es una conducta que tiene un importante arraigo, ya que no son conscientes de los peligros que esta actuación les puede suponer en un futuro. Así, por ejemplo, los investigadores Drouin, Ross y Tobin, a través de una muestra de 480 estudiantes universitarios de una universidad de Estados Unidos, han obtenido como resultados que

más del 20% de los mismos han sufrido coacciones para enviar tipos de contenido sexual a la persona con la que compartían relación sentimental, y que más del 50% de estos joven envían este tipo de fotos o videos a sus parejas (Drouin, Ross y Tobin, 2015: 201).

La principal controversia jurídica que se deriva de esta figura, radica en determinar la capacidad del menor para enviar este tipo de documentos, ya que dicha capacidad no suele coincidir con la edad que en un determinado ordenamiento se entiende que los niños y jóvenes pueden tener relaciones sexuales libremente, cuestión por otra parte, bastante compleja de determinar por el lesgilador. De forma tal, que habrá que lidiar con la tensión existente entre «la necesidad de libertad del menor para desarrollarse como persona, y la necesidad de proteger la vida privada de los menores de terceros» (Díaz Cortés, 2015: 180).

En el ordenamiento jurídico español, la edad para el consentimiento sexual entre los niños y jóvenes se sitúa en los 16 años.[26] Sin embargo, esta libertad no es plena, ya que, por ejemplo, «no se reconoce la libertad para autorizar su participación en actos pornográficos, en la elaboración del materia de ese tipo y en su ulterior distribución» (Fernández Teruelo, 2011: 120).

Cabe preguntarse si «¿se puede considerar qué tiene más connotación sexual, el que un menor de 16 años tenga relaciones sexuales, que un acto en el que dicho menor recrea en un video con escenas de actos sexuales simulados, las cuales decide compartir a través de la red» (Díaz Cortes, 2015: 181). La respuesta no es sencilla, pero la mayoría de los ordenamientos jurídicos optan por disociar los efectos de la edad para consentir libremente relaciones sexuales, con los efectos derivados de la difusión de imágenes de tipo sexual de niños y jóvenes, debido al tenebroso efecto de los pederastas. Así lo consideran otros autores al establecer que «a los efectos de los tipos relativos a pornografía infantil, deben entenderse abarcados todos los niños y jóvenes, con independencia de que concurra consentimiento sexual o no. Estos tipos se emancipan, por tanto, de la edad fijada para posibilitar el consentimiento en las relaciones sexuales» (De la Rosa Cortina, 2011: 47).

26. Artículo 183 del Código Penal: «El consentimiento libre del menor de dieciséis años excluirá la responsabilidad penal por los delitos previstos en este Capítulo, cuando el autor sea una persona próxima al menor por edad y grado de desarrollo o madurez.»

La filmación de imágenes de carácter sexual de menores y su reproducción posterior se encuentran castigadas penalmente, y en lo que afecta al *sexting* quien publique o envíe imágenes recibidas del menor de contenido íntimo, a terceras personas, puede ser condenado en España a una pena de prisión de tres meses a un año.[27]

Ahora bien, algunos estudios demuestran que muchos de los niños y jóvenes consideran que el envío de determinadas imágenes sexuales a terceros no supone un delito. En una investigación desarrollada por diversos autores estadounidenes, se obtiene como conclusión que la mayoría de los encuestados (61%) no eran conscientes de que el envío de ese tipo de contenido podría considerarse pornografía infantil en algún estado de Estados Unidos, en algunos de los cuales es un delito con graves penas de prisión. Este es el caso, de Phillip Alpert, un joven de 18 años de Florida que fue condenado por un delito grave después de que envió una foto desnuda de su exnovia de 16 años de edad, a más de 70 personas. Fue condenado a 5 años de libertad condicional, obligado a registrarse como delincuente sexual durante 25 años y expulsado de su universidad (Strohmaier, Murphy y De Matteo, 2014: 245 a 255).

Cierta doctrina opina que antes de duras leyes penales se necesita prevenir a los niños y jóvenes, y consideran que «tal vez los casos de niños *sexting* deben tratarse como cuestiones que requieren el asesoramiento de una persona calificada como un psicólogo, en lugar de ser tratado como un delito penal» (Hillman, Hooper y Raymond, 2014: 687 a 698).

LA ACTIVIDAD INTERNACIONAL EN TORNO A LA PRIVACIDAD DEL MENOR

En los últimos años, destaca una significativa actividad internacional relacionada con la preocupación por aumentar la privacidad de los usuarios en las redes sociales, fundamentalmente, en el caso de usuarios niños y jóvenes. Son, en este sentido, especialmente relevantes, por su impacto

27. Artículo 197.7 del Código Penal, en su redacción otorgada por la Ley Orgánica 1/2015 (30/3/2015): «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona».

mundial, el I Seminario Euro-Iberoamericano de Protección de Datos de Cartagena de Indias[28] y el Memorándum de Montevideo.[29]

En España se puede reseñar el Proyecto Prometeo, donde las distintas delegaciones de la Agencia Española de Protección de Datos han elaborado una serie de manuales dirigidos a los niños y jóvenes, alertándoles de los peligros de las redes sociales.

> Los manuales están específicamente trabajados para las dudas o preguntas que pueda interesar a cada grupo de usuarios, de 9 a 11 años, 12-14 y 15-17, con información para que los jóvenes usuarios sepan qué precauciones deben tomar para proteger su identidad; como no ofrecer los datos personales a cambio de servicios o regalos; no registrarse en páginas inseguras, y como saber identificarlas, o romper los mensajes en cadena y poner contraseña.[30]

Además, al igual que en el caso del Memorándum de Montevideo, se establecen una serie de recomendaciones generales, entre las que destacan la animación «a valorar el contacto 'cara a cara' con los amigos, a navegar y chatear junto con los padres y durante el tiempo pactado con ellos, así como no dar los datos personales, y ante la duda consultar».[31]

Finalmente, todo lo anterior ha contribuido, como ya se avanzó, a que la Unión Europea iniciara el 25 de enero de 2012 una 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 datos, ya que la anterior re-

---

28. I Seminario Euro-Iberoamericano de Protección de datos, analizó las repercusiones de la actividad de los menores en las redes, 26 y 28 de mayo de 2009, disponible en https://www.agpd.es/portalwebAGPD/internacional/red_iberoamericana/seminarios/2009/indexidesidphp.php.

29. Memorándum de Montevideo, Seminario Derechos, Adolescentes, y Redes Sociales en internet, 27 y 28 de julio de 2009; disponible en http://clicseguro.sep.gob.mx/archivos/Memorandum_Montevideo.pdf.

30. «Informe del Proyecto Prometeo reclama la necesidad de educar en la escuela en protección de datos», *Destrucción de Documentos*, 26 de octunbre de 2011, disponible en http://redbin.es/blog/informe-del-proyecto-prometeo-reclama-la-necesidad-de-educar-en-la-escuela-en-proteccion-de-datos.

31. Un manual específico dirigido a menores de 15 a 17 años enmarcado en el Proyecto Prometeo se encuentra disponible en http://www.madrid.org/dat_oeste/descargas/08_09/cli_prometeo/Manual_15_17_castellano.pdf.

gulación existente, es decir, la Directiva 95/46/CE, «no alcanza a regular y ni siquiera a entrever lo que serían las siguientes grandes etapas de la historia de la informática, caracterizadas por el desarrollo y la rapidez de internet, por los eficaces motores de búsqueda, o por la reciente problemática que supone el denominado internet de las cosas» (Troncoso Reigada, 2012: 72).

REFLEXIONES FINALES

En el contenido del trabajo, se ha puesto de manifiesto que el tratamiento de datos personales realizados por gigantes empresariales como Facebook y, en menor medida, Twitter, es una actividad que tiene grandes repercusiones en la sociedad, lo que ha propiciado que se ocupen del problema los ordenamientos jurídicos de todo el mundo. De la constatación del hecho anterior, se extraen una serie de reflexiones finales.

En primer lugar, el niño, el joven y el adolescente, son sujetos cuyos aspectos personalísimos son difíciles de regular, ya que, normalmente, se les niega la capacidad plena que tiene un sujeto adulto, pero se les permiten normalmente realizar determinados actos dependiendo de su nivel de madurez.

El factor determinante podría ser el de fijar una edad objetiva, a partir de la cual se entiende que el consentimiento del menor es eficaz para autorizar el tratamiento de sus datos personales por la red social. Sin embargo, tal regla no es infalible, debido al distinto grado de desarrollo de discernimiento de cada niño, lo que depende de infinitas circunstancias y no deja de plantear ciertas inseguridades legislativas.

La normativa europea sobre protección de datos personales se inclina por establecer una edad de 13 años, y si bien pudiera parece muy temprana, lo cierto es que el legislador europeo parte de un hecho fáctico indudable, que se ha puesto de manifiesto, y es que, estadísticamente, los niños a partir de los 12 años ya acceden a las redes sociales, y en la mayoría de los casos mintiendo acerca de su edad, evitando tener que recabar el consentimiento de sus progenitores o tutores legales.

En segundo lugar, no puede desconocerse la importancia decisiva de la actuación de los niños y jóvenes en todos los ámbitos de cualquier sociedad desarrollada, y mucho más en lo que respecta a sus facetas de comunicación e interrelación a través de internet.

La doctrina, en los últimos años, ha alertado sobre la importancia de proteger la privacidad de los niños y jóvenes dado que en numerosos casos han sufrido episodios más o menos graves de *sexting*, es decir, alguien ha enviado una imagen íntima suya sin su consentimiento, con el grave perjuicio moral que le puede ocasionar, o han sido objeto de acoso a través de las redes sociales.

Resulta inaplazable educar en privacidad a los niños y jóvenes que deben ser conscientes de que ciertas actuaciones divulgadas en las redes sociales pueden serles muy perjudiciales en el futuro, quedando afectados sus derechos al honor, a la intimidad y su imagen.

En tercer, y último lugar, los responsables de las redes sociales, habida cuenta de la importancia y consecuencias que lleva aparejada la intervención de los niños y jóvenes en ellas, han comenzado a introducir medidas para limitar o impedir el acceso de niños a las mismas, sin el consentimiento expreso de sus tutores en caso de que no tengan la edad fijada por la legislación. Entre estas medidas destaca la creación de perfiles espías, a través de los cuales se pueden identificar por las imágenes de los niños y jóvenes o por sus comentarios, si su edad es la legalmente establecida para prestar consentimiento a efectos de que sus datos personales sean tratados o no.

El elevado rendimiento económico que las entidades responsables de las redes sociales obtienen simplemente conociendo los datos relativos al sexo o edad de sus participantes, debería ser un aliciente para que ellas mismas elevasen el nivel de exigencia sobre el respeto de la privacidad e imagen de los niños y jóvenes.

Sin embargo, pese a todo, dada la extraordinaria dimensión del problema, que aquí tan solo se ha esbozado para buscar algo de luz entre tanta oscuridad, parece que, desde las ópticas educativas y legislativas, aún está casi todo por hacer, siendo necesario de todo punto sensibilizar a la sociedad, y, por ende, a la doctrina y a los legisladores, modesto objetivo que se ha tratado de alcanzar en las anteriores páginas.

REFERENCIAS

Acedo Penco, A. (2007). *Derecho al honor y libertad de expresión: cuestiones jurídicas actuales*. Madrid: Dykinson.

—. (2013). *Introducción al Derecho Privado*. Madrid: Dykinson.

Acquisti, A. Taylor, C., Wagman, L., (2015). «The economisc of privacy, Manuscript». *Journal of Economic*, 18:1-58.

Adsuar Prieto, Y. (2013). «La elección de ser olvidado en la red: derecho o privilegio», *Actualidad Jurídica Aranzadi*, 864: 5-8.

Almansa, A., Fonseca, O., Castillo, A. (2013). «Social Networks and Young people. Comparative Study of Facebook between Colombia and Spain». *Comunicar*, 40: 127-135. Disponible en https://goo.gl/cHZ2sR.

Andreu Martínez, M. (2013). *La protección de datos personales de los menores de edad*. Pamplona: Thomson Reuters Aranzadi.

Batuecas Caletrío, A. (2015). «El control de los padres sobre el uso que sus hijos hacen de las redes sociales», en Aparicio Vaquero (compilador), *En torno a la privacidad y la protección de datos en la sociedad de la información* (pp. 137-170). Granada: Comares.

Bauerlein, M. (2008). *The Dumbest Generation: How the Digital Age Stupefies Young Amerincans and Jeopardizes Our Future*. Nueva York: Tarcher/Penguin Books.

Berrocal Lanzarot, A. (2013). «La protección de los derechos de los menores de edad en internet». *Revista Crítica de Derecho Inmobiliario*, 739: 3371-3422. Disponible en https://goo.gl/CtC5lF.

Cebrián Herreros, M. (2008). «La web 2.0 como red social de comunicación e información». *Estudios sobre el Mensaje Periodístico*, 14: 345-361. Disponible en https://goo.gl/mkljhf.

Chen Mok, S. (2010). «Privacidad y protección de datos: un análisis de legislación comparada». *Diálogos. Revista Electrónica de Historia*, 11 (1): 111-152. Disponible en http://www.redalyc.org/pdf/439/43915696004.pdf.

Coz Fernández, J., Fojón Chamorro, E., Heradio Gil, R., Cerrada Somolinos, A. (2012). «Evaluación de la privacidad de una red social virtual». *Revista Ibérica de Sistemas y Tecnologías de la información*, 9: 59-73. Disponible en https://goo.gl/PgiuLv.

De la Rosa Cortina, J. (2011). *Los delitos de pornografía infantil. Aspectos penales, procesales y criminológicos*. Valencia: Tirant lo Blanch.

De Lama Ayma, A. (2006). *La protección de los derechos de la personalidad del menor de edad*. Valencia: Tirant lo Blanch.

Díaz Cortés, L. (2015). «La libertad sexual de los menores en el ámbito penal español: Líneas Básicas para una primera aproximación de

la información». En Aparicio Vaquero (compilador), *En torno a la privacidad y la protección de datos en la sociedad de la información* (pp. 171-186). Granada: Comares.

Díaz Gandasegui, V. (2011). «Mitos y realidades de las redes sociales». *Prisma Social*, 6: 1-26. Disponible en https://goo.gl/SVCOIi.

Drouin, M., Ross, J., Tobin, E. (2015). «Sexting: A new, digital vehicle for intimate partner agression». *Computers in Human Behavior*, 50: 197-204. Disponible en https://goo.gl/NlcJGq.

Fernández Teruelo, J. (2011). *Derecho Penal e internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes*. Valladolid: Lex Nova.

Marco Marco, J. (2010). «Menores, Ciberacoso y derechos de la personalidad». En García González (compilador), *la tutela penal de la intimidad, la integridad y la libertad sexual en internet* (pp. 85-107). Valencia: Tirant lo Blanch.

Gil Antón, A. (2015). *¿Privacidad del Menor en internet?* Pamplona: Aranzadi.

—. (2013). «La privacidad del menor en internet». *R.E.D.S*, 3: 60-96. Disponible en https://goo.gl/ghyWm8.

Gómez García, M., Ruíz Palmero, J., Sánchez Rodríguez, J., (2015). «Social learning network. Digital networks in University Education». *Edmetic*, 2 (4): 71-87.

Gordillo Cañas, A. (1986). *Capacidad, incapacidades y estabilidad de los contratos*. Madrid: Tecnos.

Grimalt Servera, P. (2013). «Los menores e internet: capacidad versus protección de la vida privada». En Ortega Doménech (compilador), *Estudios de derecho civil en homenaje al profesor Joaquín José Rams Albesa* (pp. 179-104). Madrid: Dykinson.

Heredero Campo, M. (2012). «Web 2.0: Afectación de derechos en los nuevos desarrollos de la web corporativa». *Cuadernos Red de Cátedras Telefónica*, 6: 1-40. Disponible en https://goo.gl/wOBIYi.

Hernández Martín, M. (2015). «La privacidad: Una mirada desde la economía». En Aparicio Vaquero (compilador), *En torno a la privacidad y la protección de datos en la sociedad de la información* (pp. 1-25). Granada: Comares.

Hillman, H., Hooper, C., Raymond, K. (2014). «Online child exploitation: Challenges and future research directions». *Computer*

Law and Security Review, 20: 687-698. Disponible en https://goo.gl/GcKmog.

Ibáñez Martín, J. (2013). *Estudios sobre retos éticos-pedagógicos en entornos virtuales. Análisis de la realidad y propuestas educativas*. La Rioja: Universidad Internacional de la Rioja.

inteco, Instituto Nacional de Tecnologías de la Comunicación (2009). *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*. Madrid. Inteco. Disponible en https://observatorio.iti.upv.es/media/managed_files/2009/02/13/estudio_intecoaepd_privacidad_redes_sociales_def.pdf.

Karlijn, P. (2015). «Willingness to share on commercial privacy rights and the future of data exploitation». *University of Twente, The Faculty of Behavioural, Management and Social sciences*, 2:1-20. Disponible en https://goo.gl/PxDNhx.

Lathorp, F. (2013). «El derecho a la imagen de niños, niñas y adolescentes en chile. Una mirada crítica a la luz del derecho internacional de los derechos humanos y de los estatutos normativos iberoamericanos de protección integral de la infancia y de la adolescencia». *Revista Chilena de Derecho*, 40 (3): 929-952. Disponible en https://goo.gl/AyCEZx.

Lievens, E. (2014). «Bullyng and sexting in social networks: Protecting minors form criminal acts or empowering minors to cope with risky behaviour». *Internacional Journal of Law, Crime and Justice*, 42: 251-270. Disponible en https://goo.gl/v1H8TP.

Llaneza, P. (2010). «Derechos fundamentales e internet». *Cuadernos de comunicación e innovación*: 56-59.

Marco Marco, J. (2010). «Menores, ciberacoso y derecho a la personalidad». En García González (compilador), *La tutela penal de la intimidad, la integridad y la libertad sexual en internet* (pp. 85-107). Valencia: Tirant lo Blanch.

Martínez López, F., Anaya-Sánchez, R., Aguilar-Illescas, R., Molinillo, S. (2016). *Evolution of the web*. Suiza: Springer.

Martínez Martínez, R. (2013). «Menores y redes sociales. Condiciones para el cumplimiento del artículo 13 del Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos». En Rallo Lombarte (compilador), *Derechos y Redes Sociales*. Segunda Edición. Madrid: Civitas.

Muñoz Massouh, A. (2015). «Eliminación de datos personales en internet: el reconocimiento del derecho al olvido». *Revista Chilena de Derecho y Tecnología*, 4 (2): 215-261. DOI: 10.5354/0719-2584.2015.37426.

Piñar Mañas, J. (2013). «El derecho fundamental a la protección de datos y la privacidad de los menores», en Piñar Mañas (compilador), *Redes sociales y privacidad del menor* (pp. 61-85). Barcelona: Reus.

Platero Alcón, A. (2016). «El derecho al olvido en Internet. El fenómeno de los motores de búsqueda». *Opinión Jurídica*, 15 (29): 243-260. Disponible en https://goo.gl/ghK1QP.

Plaza Penadés, J. (2008). «El derecho de protección de datos de los menores en la Comunidad Valenciana». *Derecho Civil Valenciano*, 4: 1-3.

Ravetllat Ballesté, I. y R. Pinochet Olave (2015). «El interés superior del niño en el marco de la Convención Internacional sobre los derechos del niño y su configuración en el Derecho civil chileno». *Revista Chilena de Derecho*, 42 (3): 903-934. Disponible en https://goo.gl/OCN9tM.

Figueroa García, R. (2013). «El derecho a la privacidad en la jurisdicción de protección». *Revista Chilena de Derecho*, 40 (3):859-889. Disponible en: https://goo.gl/nUHFWp.

Rovira Suero, M. (2000). *El derecho a la propia imagen. Especialidades de la responsabilidad civil en este ámbito*. Granada: Comares.

Ruiz Miguel, C. (1995). *La configuración constitucional del derecho a la intimidad*. Madrid: Tecnos.

Sabater Fernández, C. (2014). «La vida privada en la sociedad digital. La exposición pública de los jóvenes en internet». *Aposta*, 61: 1-32. Disponible en https://goo.gl/cNJbEi.

Sacco, Dena T., Argudin, Rebecca, Maguire, James, Tallon, Kelly (2010). «Sexting: Youth Practices and Legal Implications». *Cyberlaw Clinic, Harvard Law School*, 22: 1-45. Disponible en https://goo.gl/O48Piu.

Strohmainer, H., Murphy, M., De Matteo, D. (2014). «Youth Sexting: Prevelance Rates, Driving Motivations, and the Deterrent Effects of Legal Consequences». *Sex, Res Soc Policy*, 11: 245-255. DOI:10.1007/s13178-014-0162-9.

Troncoso Reigada, A. (2013). «Hacía un nuevo marco jurídico europeo de la protección de datos personales». *Revista Española de Derecho Europeo*, 43: 25-184.

Troncoso Reigada, A. (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: 61-75. Disponible en https://goo.gl/EyvxKr.

Vanderhoven, E., Schellens, T., Valcke, M. (2014). «Educating Teens the Risk on Social Network Sites. An intervention study in Secondary Education». *Comunicar*, 43: 124-132. Disponible en https://goo.gl/1xaHYH.

Vázquez de Castro, E. (2012). «Protección de datos, redes sociales y menores». *Revista de Derecho y Nuevas Tecnologías*, 29: 21-64. Disponible en https://goo.gl/hfAUMd.

Wellman, B., Hampton, K., Isla de Díaz, I., Miyata, K. (2003). «The social affordances of the internet for networked individualism». *Journal of Computer Mediate Communication*, 3: 1-28. DOI: 10.1111/j.1083-6101.2003.tb00216.x

SOBRE LOS AUTORES

Ángel Acedo Penco es Doctor en Derecho por la Universidad de Extremadura, España. Profesor Titular de Derecho Civil acreditado en la Facultad de Derecho de esa misma Universidad. Director del grupo de investigación Estudios del Derecho de España, Portugal y América Latina (GIDEPA). Coordinador en España del Comité para el Estudio y Difusión del Derecho de América Latina (CEDDAL). Su email es aacedo@unex.es.

Alejandro Platero Alcón es Licenciado en Derecho y Administración y Dirección de Empresas. Magister en Abogacía y Magister en Investigación en Ciencias Sociales y Jurídicas. Doctorando actualmente en Derecho. Investigador y docente (FPU) del Departamento de Derecho Privado de la Universidad de Extremadura. Investigador de GIDEPA (Estudios del Derecho de España, Portugal y América Latina). Su email es platero@unex.es.

Este trabajo se ha realizado en el marco del Programa Nacional de Formación de Profesorado Universitario dependiente del Ministerio de Educación y Ciencia de España. Fue recibido el 2 de agosto y aprobado el 24 de octubre de 2016.