REVISTA CHILENA
DE DERECHO Y TECNOLOGÍA

VOL. 9 NÚM. 2 (2020) • PÁGS. 105-130 • DOI 10.5354/0719-2584.2020.55333
RECIBIDO: 29/11/2019 • APROBADO: 28/7/2020 • PUBLICADO: 31/12/2020

DOCTRINA

Amenazas a la privacidad de los menores de edad a partir del *sharenting*

Threats to the privacy of young persons (minors) from sharenting

Luis Ordóñez Pineda y Stefany Calva Jiménez
Universidad Técnica Particular de Loja, Ecuador

RESUMEN En la era digital, la protección de la privacidad de los menores es uno de los debates que requieren especial atención. La sobreexposición de información personal de los menores en internet y redes sociales advierte una serie de riesgos para su privacidad, integridad, propia imagen y desarrollo de la personalidad. Desde esta perspectiva, este artículo describe la importancia del derecho a la protección de datos personales a partir de la práctica familiar de compartir cualquier tipo de información relativa a menores (imágenes, videos, etcétera). Sobre la base del concepto de corresponsabilidad digital en la familia, se plantean ejemplos de protección que concreten en la práctica la prevención y las garantías de privacidad de los menores en la web.

PALABRAS CLAVE Corresponsabilidad digital, identidad digital, menores de edad, datos personales, *sharenting*.

ABSTRACT In the digital age, the protection of the privacy of young persons is one of the debates that require special attention. The overexposure of personal information of minors on the internet and social networks warns of a series of risks for their privacy, integrity, rights to one's own image and personality development. From this perspective, this article describes the importance of the right to the protection of personal data from the family practice of sharing any type of information related to minors (images, videos, etc.). Based on the concept of digital co-responsibility in the family, examples of protection are raised that specify in practice the prevention and guarantees of privacy of young persons on the web.

KEYWORD Digital co-responsibility, digital identity, young persons, personal data, sharenting.

Introducción

El derecho fundamental a la protección de datos personales es de aquellos derechos que representan en la sociedad de la información la garantía de la privacidad, confidencialidad y seguridad digital, entre otros, y que protegen en el ámbito de la persona su información de carácter personal. Como señala la doctrina y la jurisprudencia internacional, esta libertad se constituye como un instituto de garantía de otros derechos fundamentales que puedan afectarse a través del impacto de las tecnologías de la información y comunicación en el tratamiento de datos personales.

Es evidente que en la era digital el tratamiento de datos personales exige la adopción de medidas de protección adecuadas, preventivas y pertinentes que —en el ámbito del Estado, la sociedad y la familia— aseguren un equilibrio entre el libre flujo de la información y la privacidad de los datos de las personas. Este deber tripartito que plantea el escenario de modernidad de las tecnologías es —en principio— complejo, por la variedad de exigencias, políticas, deberes y responsabilidades que el Estado, la sociedad y la familia deben asumir para materializar en la práctica la seguridad y confianza ciudadana en los entornos digitales.

En el caso de los menores de edad, sus derechos exigen adoptar cuidados y mecanismos especiales de protección que aseguren el pleno disfrute y desarrollo de su personalidad. Así, uno de los derechos de personalidad es el de identidad de los sujetos, que comprende una serie de atributos y características que permite la identificación e individualización de las personas. Como se sabe, el derecho a la protección de datos tutela a la persona en el ámbito de su información, es decir, aquélla que lo identifica o hace identificable. En este sentido, la identidad de la persona puede afectarse como consecuencia de un sinfín de contextos, entre ellos internet y redes sociales.

No es desconocido que el derecho a la identidad se encuentra especialmente incardinado con el derecho a la vida privada y el principio de autonomía de la persona. Todos ellos, garantes del reconocimiento de la dignidad humana, en la niñez y la adolescencia tienen los mismos efectos y, aún más, exigen la adopción de medidas especiales de protección por el grado de vulnerabilidad al que pueden verse expuestos. En cualquier caso, los riesgos o amenazas a los que se enfrentan los menores pueden ser impredecibles cuando media el uso de tecnologías.

Bajo estas consideraciones, este estudio pretende abordar el problema de la sobreexposición de la que pueden ser objeto los menores en internet y redes sociales a partir de la excesiva información personal que comparten los padres y responsables del cuidado de los hijos en la familia. Este planteamiento sugiere hacer una aproximación al concepto de datos personales de los menores en la sociedad de información, y así también conceptualizar el papel de la familia de cara a las innumerables amenazas que se presentan como ofensivas para la privacidad e identidad digital en la web.

En suma, si bien a la luz de la doctrina y jurisprudencia de la Corte Interamericana de Derechos Humanos se pretende enfatizar la necesidad de garantías normativas que hagan posible ejercer de manera equilibrada el derecho a la protección de datos personales en la sociedad, pretendemos precisar las condiciones en las que la familia debe garantizar una convivencia armónica en la era de la modernidad tecnológica.

El derecho fundamental a la protección de datos personales en la sociedad de la información

La conceptualización de la sociedad de la información tiene sus orígenes con el sociólogo Daniel Bellen en 1973, quien advirtió el advenimiento de la sociedad posindustrial precisando la existencia de una transformación de la economía de producción en una economía de servicios basados en el conocimiento y la información (Montesinos, 2012). Este concepto, unido a la constante implementación de herramientas tecnológicas dinámicas en el internet, ha originado que en la sociedad se establezcan nuevas conductas sociales caracterizadas, principalmente, por la interacción entre emisor y receptor en las actividades de comunicar e informar.

Al respecto, Luis González de la Garza —citado por Montesinos— afirma que «las comunicaciones en internet tienen una naturaleza bidireccional, las cuales hacen posible la participación ciudadana en diversas esferas de interés» (Montesinos, 2012: 177).

> Es evidente que la sociedad de la información se ha construido sobre la base del desarrollo de las tecnologías y procesos encaminados a erradicar la brecha digital, en que la ciudadanía ha adquirido la función de comunicar, informar, responder, receptar o en definitiva interactuar en internet en torno a la información que sea de su interés. No obstante, existen tensiones cuando aquella información objeto de la interacción afecta la privacidad, buen nombre, desarrollo de la personalidad, imagen, etcétera, de la persona, por cuanto existe desconocimiento sobre los riesgos que representan difundir grandes volúmenes de información en plataformas digitales (Calva, 2020: 8).

La información, como precisa Troncoso (2010: 32), que una persona «no ha querido revelar afecta seriamente a la forma en que ésta se desenvuelve normalmente en la sociedad, la manera en que es vista por sus familiares, por sus vecinos, por sus compañeros de trabajo». Así también, Gil (2013: 175) advierte que los datos concernientes a una persona no son algo anecdótico, sino que representan el registro de su vida, reflejan características, opciones vitales, debilidades, figura humana, gestos, aptitudes etcétera.

En general, los datos de carácter personal revelan aquellas característica, aspectos y cualidades innatas que corresponden a la individualidad y personalidad de un

sujeto, lo cual implica una serie de deberes y limitaciones con respecto al derecho a la protección de datos. Además, considerados como una fuente de valor económico y empresarial en la sociedad de la información, al ser organizados con aquellas características propias de un individuo (perfiles de personalidad), los datos personales proveen de conocimiento a terceros con el objeto de implementar la tomar decisiones tanto en el ámbito comercial como delictivo.[1]

Según la doctrina y normativa internacional, los datos personales cuentan con una categoría de sensible o especialmente protegidos, respecto de aquella información que debería concretar un mayor cuidado, como informes médicos, religión, antecedentes penales y otros. Así, se plantea desde distintas perspectivas la necesidad de proveer adecuados niveles de protección que impidan posibles discriminaciones a partir tratamientos ilícitos relacionados con la intimidad, el buen nombre, la imagen o la dignidad (Calva, 2020). Por ejemplo, como señala la doctrina, en el caso de los menores de edad:

> 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 (Acedo y Platero, 2016: 64).[2]

Conviene advertir que, según Serrano y Rebollo, al referirnos a protección de datos no existe información irrelevante, por lo que toda información requiere de protección o cuidado, pues en el marco de su uso, los datos de carácter personal puede convertirse en delicada, afectando los aspectos más íntimos de las personas y generando un verdadero peligro. Sin embargo, existe información que por su naturaleza se la puede establecer como sensible, por lo que se necesita de un tratamiento especial como lo es la información sobre «el origen racial o étnico, las opiniones políticas,

1. Como precisa el Reglamento (UE) 2016/679 de Protección de Datos Personales, «las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de *cookies* u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas».

2. En este sentido, conviene destacar que el Reglamento (UE) 2016/679 estima que «los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño».

filosóficas, religiosas, la afiliación sindical, la vida sexual, el estado de salud, la situación patrimonial, la situación financiera, las condenas penales, etcétera» (Serrano y Rebollo, 2008: 162).

La protección de datos personales es un derecho fundamental inherente a cada ser humano, a fin de que éste se pueda desarrollar en condiciones óptimas en su entorno. En cualquier caso, por el universo que representa internet y el pleno ejercicio de derechos relacionados con la libertad de expresión, la protección de datos se ha visto limitada, en especial con los menores de edad, mismos que según normativa nacional e internacional deben contar con una protección prioritaria por ser más susceptibles a vulneraciones.

Al respecto, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos de 2017 señala que «en el tratamiento de datos personales concernientes a niñas, niños y adolescentes, los Estados Iberoamericanos privilegiarán la protección del interés superior de éstos […] para que busquen su bienestar y protección integral».[3]

Tomando en cuenta que en la actualidad el acceso a las tecnologías es muy frecuente en la niñez y la adolescencia, el Memorándum de Montevideo de 2009 advierte además que la diversidad de sistemas de comunicación «ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros—».[4]

En efecto, los datos personales de la niñez y adolescencia en plataformas virtuales o internet son aquéllos que permiten de manera directa o indirecta individualizar y

3. La Red Iberoamericana de Protección de Datos (RIPD) concretó en 2017 la aprobación de este instrumento, que puede considerarse como una ley modelo, por cuanto expone disposiciones relativas a los principios, definiciones, ámbito de aplicación, derechos y obligaciones, ejercicio de los derechos arco, transferencias internacionales de datos personales, medidas proactivas, autoridades de control, reclamaciones y sanciones y mecanismos de cooperación internacional.

4. El «Memorándum de Montevideo sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes» es un documento que adopta una serie de recomendaciones dentro de un seminario de trabajo llevado a cabo en Montevideo los días 27 y 28 de julio de 2009. Fue convocado por el Centro Internacional de Investigaciones para el Desarrollo de Canadá, en donde se concentraron los principales representantes gubernamentales de Brasil, Canadá, España, Uruguay, Perú, Ecuador, Colombia, Argentina y México. Teniendo como referente normativo fundamental la Convención de Naciones Unidas sobre los Derechos del Niño (CDN), su principal objetivo fue exponer las problemáticas derivadas de la protección de los derechos fundamentales de los niños, niñas y adolescentes a partir de los riesgos que suponen la sociedad de la información y conocimiento. Como se señala en este documento, las recomendaciones formuladas son «una contribución para que los diversos actores involucrados de la región se comprometan con el tema para extender los aspectos positivos de la sociedad de la información y conocimiento, incluyendo internet y las redes sociales digitales, así como prevenir aquellas prácticas perjudiciales que serán muy difíciles de revertir, así como los impactos negativos que las mismas conllevan».

determinar su imagen y personalidad, lo cual supone un gran peligro (Calva, 2020). Por esta razón, a través del principio del interés superior se busca tutelar la integridad y desarrollo pleno de los menores de edad. Al caso, María Mercedes Serrano Pérez —citado por Hidalgo— señala que:

> Con el derecho a la intimidad se protege el espacio inmaterial de desarrollo de aspectos de la vida privada tanto frente a intromisiones no consentidas, como a la divulgación de lo conocido por medio de la intromisión. Por ello, el derecho a la intimidad se traduce también en un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público (Hidalgo, 2016: 739).

Así también, Miguel Ángel Davara Rodríguez —citado por Conde (2005: 20)— afirma que es necesario una protección jurídica de la intimidad, como «un límite a la utilización de la informática y las comunicaciones ante la posibilidad de que se pueda agredir a la intimidad de los ciudadanos», y que por el mal manejo de la información se pueda coartar el pleno ejercicio de sus derechos. En todo caso, conviene advertir que «no basta con la consagración explícita a nivel de garantía constitucional de este derecho, si no se establecen mecanismos efectivos que aseguren el respeto y protección de la privacidad en general» (Herrera Carpintero, 2016: 90).

Si bien el derecho a la intimidad tiene como finalidad que aquellos aspectos de la vida privada permanezcan en esta esfera, pues hacer pública información personal privada de una persona en medios telemáticos constituye una violación a más derechos; en el caso de los menores de edad, la publicidad de su información puede suponer mayor gravedad. Por ello, es importante recalcar que la protección de datos personales debe concretarse «sin que se afecte su dignidad como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un espacio privado» (Memorándum de Montevideo, p. 4).

Así, es fundamental que la concreción de las garantías para la protección de datos personales se reconozca en el ámbito constitucional y sectorial, pero también es esencial que para su justiciabilidad concurra la acción tripartita del Estado, la sociedad y la familia, ya que, como se verá más adelante, «ante la excesiva cantidad de datos personales y sensibles que pueden solicitar las redes sociales en la etapa de registro, sumado a la ignorancia del usuario promedio respecto a las implicancias que conlleva compartirlos, los ataques informáticos han aumentado» (Herrera Carpintero, 2016: 99).[5]

5. Como señala el Memorándum de Montevideo, «el derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, para asegurar la autonomía de los individuos, decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias, en dicha esfera personal».

Así, en el caso del tratamiento de datos personales de menores, conviene precisar que «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» (Acedo y Platero, 2016: 77) y que, en cualquier caso, quienes ejercen su representación tienen el deber y la obligación de respetar.

Respecto de la importancia del respeto del derecho al honor, Marcela Basterra —citado por Lathrop— advierte:

> Es el derecho a ser respetado ante sí mismo y ante los demás, con fundamento en la dignidad personal; comprendiendo en ello el honor subjetivo, que es la autovaloración, es decir, el íntimo sentimiento que cada persona tiene de la propia dignidad y la de su familia; y el honor objetivo, que es el buen nombre o la buena reputación adquiridos por la virtud y el mérito de la persona o de la familia que se trate, dentro del ámbito social en el que se desenvuelve (Lathrop, 2013: 933).

Al no existir un adecuado tratamiento de la información, se expone a los menores de edad a diversos peligros, y por ende a la vulneración de derechos como el de la privacidad o intimidad, que tiene como función mantener en secreto o de manera privada aquella información que el titular no desea que sea pública. Así también, el derecho al buen nombre u honor, que se refiere a la autovaloración o valoración de terceros hacia una persona, categorizándola de manera específica según su percepción. De cualquier modo, si bien en muchos casos los menores no son conscientes del tipo de información que comparten a terceros, los peligros relativos tanto a su integridad como identidad digital permanecen a través del tiempo.

En las redes sociales, este consentimiento es otorgado —sin saberlo— por los niños y jóvenes que acceden a éstas 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 rara vez se llegan a prever (Acedo y Platero, 2016: 73).

Asimismo, si la percepción de terceros hacia un niño o adolescente es negativa, podrá influir en su identidad, pues —como es de conocimiento general— los menores de edad se encuentran en pleno desarrollo y han adquirido su condición de grupo de atención prioritaria por no poder representarse a sí solos o no contar con una identidad definida. Por este motivo en particular, los datos personales de la niñez y adolescencia deben estar revestidos de mecanismos que aseguren la protección de su identidad digital, teniendo como encargados de esta tutela al Estado, sociedad y familia.[6] Como advierte la doctrina sobre el problema que plantean las tecnologías

6. Como precisa la Corte Interamericana de Derechos Humanos, «la protección de los niños en los instrumentos internacionales tiene como objetivo último el desarrollo armonioso de la personalidad de aquéllos y el disfrute de los derechos que les han sido reconocidos. Corresponde al Estado precisar

respecto de la protección de la identidad de los menores en la red, es fundamental «la labor de los padres, tutores y profesores que han de concienciar a los menores de la importancia de gestionar correctamente la identidad en internet, de practicar el *egosurfing* (buscarse a sí mismo en la red)» (Davara Fernández, 2017: 76).

Sobre la importancia del derecho a la identidad, Rebollo y Saltor (2013: 120) refieren que este derecho «es la forma en la que una persona busca presentarse ante terceros y a la sociedad […] y cuando los datos personales publicados son sensibles se afecta al derecho a la identidad personal». Bajo esta conceptualización, puede decirse que la *identidad digital* se refiere al conjunto de datos, características o información subida a internet capaz de individualizar, identificar o hacerla identificable a la persona; de manera específica, puede ser esta persona un menor de edad.

Además, el derecho a la identidad digital, es decir, la manera en que un individuo se presenta a terceros en internet, la debe plantear y ejercer el titular del derecho. No obstante, al tratarse de menores de edad, quienes han adquirido el ejercicio del mencionado derecho en la sociedad de la información han sido los padres o familiares, mismos que, con sus prácticas de interacción en internet con imágenes, videos, comentarios y más de sus hijos, ya establecen la identidad digital sin tomar en cuenta su opinión o consentimiento sobre el tipo de información que quieren que los caracterice a lo largo de su vida.

Así, es imprescindible recordar que la información almacenada en la web perdura por siempre, pese a que el primer emisor borre la información. Por ello, en el caso de la sobreexposición de los menores en internet y redes sociales, hay que tomar en consideración que casi siempre «no se tiene en cuenta que la masividad hace que estas imágenes y comentarios puedan, eventualmente, ser vistas por cualquiera. Es importante conocer dónde está el límite, cuánto y qué se debe compartir» (Otero, 2017: 412).

Como sostiene Eberlin (2017: 258):

> Aquella información que se publica en la web puede provocar grandes impactos desde la infancia hasta la vida adulta, pues se deja una huella digital, misma, que le perseguirá durante toda su existencia, y como lo explica [Stacey Steinberg], al publicar información personal, una imagen un audio, video u otro se puede exponer al menor de edad a comentarios o reacciones que se los consideraría como vergonzosos.

El derecho a la privacidad, buen nombre, imagen, dignidad, identidad, etcétera, son bienes jurídicos tutelados en la sociedad de la información y del conocimiento

---

las medidas que adoptará para alentar ese desarrollo en su propio ámbito de competencia y apoyar a la familia en la función que ésta naturalmente tiene a su cargo, para brindar protección a los niños que forman parte de ella» (Opinión Consultiva 17/2002, p. 60).

por el derecho a la autodeterminación informativa, por cuanto constituye información de carácter personal que vincula o asocia a una persona en plataformas virtuales. Así, como precisan Millán y Peralta (1995: 211), el derecho a la autodeterminación

> se construye a partir de la noción de intimidad (*vie privée*, *privacy*) y se encamina fundamentalmente a dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales: es, pues, respuesta a exigencias concretas de la convivencia actual. Se plantea, por tanto, como una cuestión previa su diferenciación del derecho a la intimidad.

En síntesis, el derecho a la protección de datos o a la autodeterminación informativa es la facultad que tiene la persona para ejercer el control de la información que se vincule con ella, cuyo objeto es proveer de una protección integral frente a los peligros que se evidencian en la sociedad de la información. De esta manera, la familia representa el núcleo fundamental en que este derecho exige medidas urgentes y especiales de cara al desarrollo de las tecnologías.

Conviene resaltar que, en materia de niñez y adolescencia, la protección de datos personales exige, además, una labor proactiva de los Estados, con especial énfasis en el desarrollo de instrumentos regionales o comunitarios que permitan asegurar un marco homogéneo y equilibrado.[7] Así, de los ya citados, en el ámbito europeo destacan algunos instrumentos comunitarios que han concretado un adecuado tratamiento de la información en internet.

En la Unión Europea existe un marco común que reconoce, a través de la Carta de Derechos Fundamentales, a la protección de datos como un derecho fundamental (artículo 8.1), bajo el cual toda persona «tiene derecho a la protección de los datos de carácter personal que la conciernan». Asimismo, el Reglamento (UE) 2016/679 de Protección de Datos Personales (artículo 1.2), en su objeto «protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales».

Ahora bien, en lo que corresponde a los derechos relativos a los menores de edad, tanto la Carta de Derechos fundamentales (artículo 24.1) como el Reglamento (UE) 2016/679 (artículo 57.1) coinciden, respectivamente, que los menores «tienen derecho a la protección y a los cuidados necesarios para su bienestar» y, a su vez, que los Estados, a través de las autoridades de control y supervisión, deben garantizar que la tutela de ese bienestar se promueva mediante «la sensibilización del público y su

7. Como precisa el Memorándum de Montevideo: «Los organismos multilaterales deberán incluir en sus documentos, directrices o recomendaciones a las niñas, niños y adolescentes como sujetos especialmente protegidos y vulnerables respecto del tratamiento de sus datos personales. Asimismo, deberán enfocar esfuerzos para promover o fortalecer una cultura de protección de datos en las niñas, niños y adolescentes».

comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención».

De la misma manera, en el ámbito europeo, un ejemplo de regulación en materia de protección de datos personales es la normativa española. Considerada como una de las primeras constituciones a nivel global en reconocer las limitaciones de la tecnología en la vida de las personas (artículo 18.4), la Carta Magna española garantiza que «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». Así, en materia de protección de datos de los menores, la actual Ley de Protección de Datos Personales y garantía de los Derechos Digitales (artículo 84.1) precisa:

> Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información, a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

En este orden, Solé, sobre el marco legal español, afirma que:

> En el marco legal vigente, ni el menor ni sus representantes legales pueden consentir actuaciones contrarias a los derechos reconocidos, pues ese consentimiento será ineficaz para excluir la lesión del derecho si puede implicar menoscabo para la honra o reputación, o ser contraria a sus intereses, con lo que su margen de decisión sobre estos derechos es mínimo y limitado por criterios objetivos. Hasta este punto llega la protección de los derechos fundamentales al honor, a la intimidad y a la propia imagen del menor. Y así se concreta, en este caso, el principio del interés superior del menor (Solé, 2015: 204).

Por otra parte, en el contexto interamericano, la Convención Americana sobre Derechos Humanos (artículo 11) señala que se deberá proteger la honra y la dignidad, en particular si se trata de un niño, niña o adolescente, bajo el principio del interés superior del niño. Por esto, se limita la discrecionalidad de los juzgadores, a fin de que se resuelva siempre en favor de los menores de edad, erradicando de manera definitiva la doctrina de situación irregular.

Cabe mencionar que en el preámbulo de la Convención Americana de Derechos de los Niños (CADN) señala la prevalencia del interés superior del niño al afirmar que éstos requieren cuidados especiales, mientras que el artículo 19 señala que el Estado debe adoptar las medidas necesarias para proteger a los menores estando en cuidado de sus padres o representantes. La CADH, en su artículo 19, en concordancia con el anterior cuerpo normativo, afirma que los niños deberán contar con una protección específica para sus necesidades, tomando en cuenta su vulnerabilidad, debilidad, inmadurez o inexperiencia.

A diferencia del marco europeo, en el ámbito interamericano no existen instrumentos regionales que deriven, obligatoriamente, en los sistemas jurídicos de cada Estado en la aplicación de principios o estándares de protección de la información personal, menos aún en el caso de la niñez y la adolescencia. En cualquier caso, debe destacarse el modelo de regulación que proponen los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. En el caso de la protección de datos de los menores, esta propuesta plantea que

> los Estados iberoamericanos promoverán en la formación académica de las niñas, niños y adolescentes, el uso responsable, adecuado y seguro de las tecnologías de la información y comunicación y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

En este contexto, en materia de protección de datos de los menores, en nuestro ámbito regional las únicas referencias a modo de recomendaciones, directrices, iniciativas regulatorias y guías legislativas son el Memorándum de Montevideo y los Estándares de Protección de Datos Personales para los Estados Iberoamericanos. Queremos resaltar, además, la importancia de la Opinión Consultiva 17/2002 de la Corte Interamericana de Derechos Humanos, por la cual se establecen algunas precisiones sobre la condición jurídica y derechos relativos a los menores.[8]

Finalmente, en esta parte precisamos advertir la importancia del consentimiento en el tratamiento de datos personales de los menores. Como se analizará más adelante, muchos de los atentados a la privacidad, identidad digital, desarrollo de la personalidad y a la propia imagen de los menores proceden de la sobreexposición que hacen los padres en redes sociales.

> Nos viene a la cabeza la tendencia del «oversharing» de los padres y es que, si bien es cierto que en la Sociedad de la Información y del Conocimiento en la que vivimos el gusto por lo social y por compartir todo tipo de información —personal o no— en forma de imagen, vídeo o audio es generalizado, la realidad es que todo ello ha determinado que algunos padres hayan caído en lo que se ha dado en denominar el «oversharing» —palabra inglesa que describe el hecho de compartir todo tipo de información personal, prácticamente sin límite (Davara Fernández, 2017: 23).

8. La Opinión Consultiva 17/2002, del 28 de agosto de 2002, solicitada por la Comisión Interamericana de Derechos Humanos, por la cual se manifiesta la «Condición jurídica y derechos humanos del niño», se orienta a establecer «la interpretación de los artículos 8 y 25 de la Convención Americana, con el propósito de determinar si las medidas especiales establecidas en el artículo 19 de la misma Convención constituyen "límites al arbitrio o a la discrecionalidad de los Estados" en relación a niños, y […] formulación de criterios generales válidos sobre la materia dentro del marco de la Convención Americana» (página 3).

Según Azurmendi (2018) el menor está desprotegido ante el riesgo de que el adulto que le tutela. Precisamente prevaliéndose de su ascendencia, vulnere la privacidad del menor, vendiendo o difundiendo sus datos. Sería una posibilidad que podría abordarse desde las responsabilidades de la tutela legal del menor, en el sentido de que se previeran sanciones por este tipo de conducta abusiva.

Hay que tomar en cuenta que para la difusión de datos personales se deberá contar con el previo consentimiento de su titular o sus representantes como lo son los padres de los menores de edad (Calva, 2020). Sin embargo, se ha evidenciado que los adultos, padres o quienes ejercen la representación o patria potestad, valiéndose de su figura y en gran medida por desconocimiento, no garantizan una protección adecuada de los datos de los menores, generando de esta manera vulneración a su privacidad y otro tipo de riesgos.

> En el mismo sentido, conviene observar que, para asegurar, en la mayor medida posible, la prevalencia del interés superior del niño, el preámbulo de la Convención sobre los Derechos del Niño establece que éste requiere «cuidados especiales», y el artículo 19 de la Convención Americana señala que debe recibir «medidas especiales de protección». En ambos casos, la necesidad de adoptar esas medidas o cuidados proviene de la situación específica en la que se encuentran los niños, tomando en cuenta su debilidad, inmadurez o inexperiencia (Opinión Consultiva 17/2002, p. 62).

Con referencia a este aspecto, los menores de edad, por su inexperiencia o inmadurez, deben contar con una protección de carácter prioritaria y especial, en que la familia, la sociedad y el Estado —bajo el interés superior del niño— son los encargados de proveer de una adecuada protección de sus datos personales en internet o la sociedad de la información. Por ello, es esencial destacar que «padres, profesores y demás agentes que traten con menores desarrollen una labor de concienciación y sensibilización sobre un uso adecuado —y cumpliendo las normas— de las redes sociales» (Davara Fernández, 2017: 19).

En la presente época, no se puede hablar de ausencia de normativa que vele por la protección de datos personales. No obstante, por el hecho de que la sociedad de la información sea de cierta manera nueva o cambiante por estar en constante construcción y por desconocimiento de los padres o familiares de los menores de edad, las consecuencias y amenazas sobre el tratamiento de la información personal de los menores pasan inadvertidas.

Amenazas digitales y sobrexposición de los niños, niñas y adolescentes en la red

El Reglamento (UE) 2016/679 señala que «la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa». Las redes sociales no son malas o peligrosas, lo peligroso es el uso inadecuado que se les dé, como en la publicación excesiva de la información en espacios informáticos, que facilita que terceras personas usen la información para fines ilícitos (Herrera Carpintero, 2016: 95).

Las redes sociales en apariencia ofrecen muchos beneficios a los padres cuando éstos comparten información sobre su vida o la vida de sus hijos, ya que amigos, familiares y otras personas pueden, por medio de comentarios de validación, reacciones como un «me gusta» o compartiendo, reflejar un estímulo que alienta a los padres a seguir publicando información de sus hijos (Steinberg, 2017: 846).

La acción de los padres de compartir información pormenorizada de sus hijos en internet a través de redes sociales se la ha denominado *sharenting* (Otero, 2017: 1). Esta práctica se la considera como un potencial peligro debido a que la información publicada por los padres es constante y excesiva, mostrando cada accionar de sus hijos, como el lugar donde estudian, a dónde se van de paseo o cuáles son sus gustos. Es decir, todo tipo de información capaz de individualizar a una persona, la cual debería permanecer en la esfera de lo privado.

Los padres, en representación de la familia y bajo el principio de corresponsabilidad, son considerados como los defensores naturales de la identidad digital de sus hijos. No obstante, no siempre cumplen con este deber, pues asegurando que tienen el derecho de publicar información de sus hijos mediante un ejercicio extralimitado de la patria potestad, olvidan los principios fundamentales de consentimiento e interés superior del niño. Como hemos señalado, a la luz del principio del interés superior del niño, se entiende que todas las actuaciones realizadas por el Estado, sociedad y familia serán en beneficio de los menores, y por ende esa corresponsabilidad se verá presente en medios digitales. Sin embargo, con la publicidad masiva de información personal de niños, este principio se ha visto limitado.

Al respecto, Steinberg (2017: 843) señala que «las divulgaciones en línea por parte de los padres hacia los hijos pueden ser una fuente potencial de peligro, ya sea intencionalmente o no». Así, se genera un impacto a derechos fundamentales como la intimidad e identidad, ya que cualquier persona en el mundo que cuente con internet y acceso a dicha información, tendrá la facultad de usarla según sea su interés o beneficio.

Los peligros generados por la sobreexposición de información de los menores de edad en redes sociales son inimaginables. En lo principal, se puede identificar el

menoscabo de su identidad e intimidad reflejándose en delitos como pornografía infantil, ciberacoso, *cyberbullying*, cibersuplantación de identidad y más (Calva, 2020).

La violencia se adapta a la realidad social que se le presente (Castro, 2013: 61) y el entorno digital no es la excepción, ya que el objetivo del ciberacoso es causar afectación en el menor de edad empleando las tecnologías. De conformidad con lo señalado por Steinberg, una de las fuentes empleadas para obtener información vergonzosa es el perfil de los padres del niño al que le quieren causar el daño, debido a que los padres publican todo tipo de información de los titulares.

Para la Agencia Española de Protección de Datos (AEPD), «cuando se acosa a alguien a través de internet, se denomina ciberacoso, o *ciberbullying* si se produce entre menores. Además de los daños que pueden ser devastadores para quien los sufre, se puede cometer un delito cuyas consecuencias […] pueden repercutir en sus padres».[9]

De esta manera, Troncoso (2010: 1714) advierte que «es especialmente grave la posibilidad que ofrecen las redes sociales para llevar a cabo el *cyberbullying* –acoso a través de las tecnologías de información–, que convierte la vida de algunos jóvenes o de profesores en una auténtica pesadilla». En el mismo contexto, García menciona que es la «acción agresiva e intencional desarrollada por un grupo o individuo, usando formas electrónicas de contacto repetidas veces a lo largo del tiempo contra una víctima que no puede defenderse fácilmente, ocasionando un desequilibrio de poder» (García-Atance, 2017: 1.290).

El *cyberbullying* en su mayoría es practicado por personas que han conocido al menor de edad con anterioridad, y al llevar a cabo esta conducta se afecta directamente a la dignidad de la persona, buen nombre e imagen. Además, en algunos casos, se asocia con el suicidio de adolescentes, como lo refleja un estudio presentado en la Academia American de Pediatría (AAP) y la Conferencia Nacional de Exposiciones en Nueva Orleans en el año 2012 (Castro, 2013: 64).

> En efecto, si nos referimos al ámbito de los menores, no nos resulta extraño que en ambientes escolares este tipo de supuestos de etiquetado de fotografías o su manipulación suele ser utilizado para ridiculizar a compañeros o profesores. Pero además, son cada vez más habituales los supuestos de *ciberbullying* o acoso escolar por vía telemática, y en muchos de los casos se utilizan fotografías o el denominado *happy slapping*, conducta consistente en la grabación de imágenes o videos a través de los móviles para posteriormente incluirlas en plataformas de contenidos como *Youtube* y *Myspace*, y cuyo fin no es otro que ridiculizar o vejar a la víctima, cuando ésta se sitúa en determinadas actitudes, al verse sorprendida o agredida por un conjunto de estudiantes ya sean o no menores, y ser grabadas estas imágenes (Gil, 2013: 103).

9. «Protección de datos y prevención del delito», Agencia Española de Protección de Datos, p. 6, disponible en https://bit.ly/3nRc5a6.

Como se mencionó, el *cyberbullying* no es el único peligro al que se encuentran expuestos los menores de edad como resultado de la publicación en masa de información personal. Otra de las actividades realizadas es el *morphing* o *warping*, que García define como:

> Una técnica de metamorfosis que no tiene en su origen ninguna finalidad dañina, se trata de retocar secuencialmente la imagen hasta transformarla en otra totalmente diferente, considerándose un arma muy preciada en el mundo artístico para la confección de imágenes no existentes previamente. Sin embargo, en el objeto de estudio que nos ocupa, su finalidad es absolutamente destructiva e intencional de causar daño al menor desprestigiando su imagen, convirtiéndole en objeto de burla (García, 2017: 1.294).

Otro peligro al que se expone al menor de edad por inadecuado manejo de la información es la pornografía infantil, para lo cual Alarcón concluye que «es toda representación visual de índole sexual real, de menores de edad, a través de un sistema informático, con la finalidad de producirla, ofertarla, difundirla, adquirirla o poseerla» (Alarcón, 2015: 23). En muchas ocasiones se origina con la publicación de imágenes en medios telemáticos por los familiares o menores de edad sin un sentido sexual. Sin embargo, con el mal manejo y manipulación de terceros cambian el contexto y afecta la integridad del menor.

El *grooming* es otra de las conductas a las que se encuentran expuestos los niños, niñas y adolescentes, ya que, «es el acoso a menores en línea o ciberacoso» (Fernández Sousa, 2015: 7). Asimismo, García (2017: 1.292) añade: «El *grooming* se constituye por el acercamiento de un adulto hacia un menor de edad por internet o cualquiera de las TIC, a fin de ganar su confianza para posterior abusar sexualmente de él». En todo caso, estimando que esta amenaza para los menores puede derivarse de contenidos íntimos que obran en internet y redes sociales. Hay que resaltar que la sobrexposición de información (fotografías, videos, geolocalización) puede coadyuvar y limitar el derecho de los menores en la red.

La conducta del *sharenting* se incrementa cuando existe la «hipersexualización infantil», que es la simulación de «mini adultos», lo que hace a su vez que estas imágenes sean empleadas para pornografía infantil.[10]

La AEPD también refiere sobre los peligros que presenta el inadecuado manejo de la información, al señalar:

> Los casos más típicos son la suplantación de identidad en perfiles de redes sociales, que normalmente consisten en la creación de un perfil falso en nombre de la víctima bajo el que se comparte contenido o se crea un daño a la imagen de la

10. Romina Tarifa, «Alerta para los padres: *Sharenting* y pornografía infantil», *Injujuy*, 29 de julio de 2019, disponible en https://bit.ly/33gwgqd.

> persona suplantada […], la cual puede obedecer a diferentes motivos, como socavar o destruir la reputación del suplantado, coaccionarle, acosarle o estafarle… Muchas veces los autores pueden pensar que sólo le están gastando una broma, sin ser conscientes del grave daño que causan a la persona suplantada.[11]

Cada una de estas conductas hechas por medio de las plataformas virtuales por un grupo o una persona tienen como fin lesionar la imagen, buen nombre, intimidad, dignidad, etcétera, de los niños, niñas y adolescentes, derechos que afectan en el ámbito inmaterial y material del ser humano, por lo que, sin duda, según todos los cuerpos normativos, se debe velar por que se limite o filtre aquella información que se publica en el internet.

No lejos de la realidad, de conformidad con el estudio de 41 casos analizado por Castro, el *cyberbullying* genera la violación de varios derechos de un niño y por su condición de inmadurez predispone a que tengan otras dificultades como la depresión, como respuesta del constante hostigamiento, que cuando no cuenta con tratamientos médicos, se ve vinculada con el suicidio (Castro, 2013: 64).

Frente a estos casos, en los que los menores de edad se ven afectados por la sobreexposición de información en redes sociales, al ser los padres quienes generan esta práctica se estaría hablando del incumplimiento del deber objetivo de cuidado y, por ende, de la corresponsabilidad que le es inherente a la familia.

Es necesario manifestar que no sólo la familia es la encargada de proteger a los menores de edad sino el Estado, la sociedad y la familia con un deber tripartito. Sin embargo, la familia o en este caso los padres son los que por su condición pueden disponer de primera mano de todo tipo de información personal de sus hijos en cualquier medio, además de que son los más cercanos para controlar que el manejo de las redes sociales sea responsable, considerándosela de esta manera el núcleo central para el cuidado, formación y protección de sus hijos (Calva, 2020).

El deber de corresponsabilidad digital: El papel de la familia

La evolución de las tecnologías de la información y comunicación ha llegado a significar una potencial amenaza para la defensa de los derechos fundamentales de los niños, niñas y adolescentes. En lo que refiere al derecho a la protección de datos personales, el uso de las tecnologías plantea no sólo la exigencia de un marco de regulación apropiado, sino también la observancia de los deberes y responsabilidades que corresponden a la familia, toda vez que internet y redes sociales convierten a niños y adolescentes en blancos fáciles de quienes se aprovechan de la información personal registrada en la web, lo que da lugar al *grooming*, *ciberbullying*, *sexting*, etcétera, sobre

11. «Protección…».

todo como resultado de la práctica de compartir información personal desde el entorno familiar, denominada s*harenting*.

Si bien la sociedad es consciente de la información que comparte en la web, debe tenerse en cuenta que «el exceso de información compartida en estos espacios sociales facilita que terceras personas, sean naturales o jurídicas, utilicen dicha información con fines ilícitos» (Herrera Carpintero, 2016: 95). El panorama se vuelve más complejo cuando, conscientemente, la familia comparte gran cantidad de información que corresponde a los menores sin tomar en cuenta los riesgos que esto implica, tanto en el presente como en el futuro, para la privacidad en la web.

En este orden de ideas, *a contra sensu* de las bondades que se desprenden del uso de tecnologías, el acercamiento a internet y redes sociales «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» (Acedo y Platero, 2016: 66).

Como hemos mencionado, en la doctrina y jurisprudencia internacional el derecho a la protección de datos se distingue por su carácter instrumental, materializado en la garantía de otros derechos fundamentales. Mientras que, en el caso de la niñez y la adolescencia, a partir del principio de interés superior, exige la adopción de medidas que concreten una protección especial, por cuanto, desde situaciones cotidianas que se desprenden del uso ilícito de la información personal, se puede desembocar en afectaciones a la imagen, desarrollo de la personalidad y dignidad personal.

Así, conflictos jurídicos que resultan de actos de odio, discriminación, extorsión y acoso sexual representan algunos de los principales peligros en una sociedad en que la información personal —todo aquello que pueda identificar o hacer identificable a una persona— requiere especial atención por la sobrexposición a la que pueden ser sujetos. Por ello, es conveniente destacar la importancia de la corresponsabilidad digital, especialmente en la familia.

En sentido general, entendemos que el concepto de corresponsabilidad en materia de protección de datos tiene una función tripartita, derivada «del deber que se impone al Estado, la sociedad y la familia. Se encamina a adoptar medidas —sociales, políticas y jurídicas— para la plena vigencia, ejercicio, garantía, protección y exigibilidad de los derechos de los titulares de la información personal» (Ordóñez, 2018: 388). Ahora bien, al ser la familia la institución y núcleo fundamental para el desarrollo de los menores, capaz de satisfacer las necesidades materiales, afectivas y psicológicas, «la importancia de abordar el fenómeno tecnológico frente al tratamiento de la información personal exige analizar las condiciones necesarias que en la práctica deben desarrollarse para efectivizar la tutela de este derecho fundamental» (Ordóñez, 2018: 391).

En este marco, en la parte final de este estudio pretendemos desarrollar las condiciones que corresponden a la familia, con el objeto de concretar un modelo de co-

rresponsabilidad digital frente al tratamiento de datos personales de los menores en entornos digitales. Para este fin, tomaremos como referencia la Opinión Consultiva 17/2002, solicitada por la Comisión Interamericana de Derechos Humanos, por la cual la Corte Interamericana de Derechos Humanos establece la «Condición jurídica y derechos humanos del niño». Así también, el Memorándum de Montevideo «Sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes» significa un instrumento regional importante a partir de las recomendaciones respecto de la la protección de datos personales de la niñez y adolescencia.

La Corte Interamericana de Derechos Humanos conceptualiza a la familia como el núcleo central de protección y la define como «el ámbito primordial para el desarrollo del niño y el ejercicio de sus derechos» (Opinión Consultiva 17/2002, p. 86).[12] En la era digital, esta definición conlleva el aseguramiento de un desarrollo equilibrado, de manera que su información personal no sea objeto de intromisiones ilegales o arbitrarias. Por esto, el papel de la familia es fundamental «en el proceso de educación sobre el uso responsable y seguro de herramientas como internet y las redes sociales digitales y en la protección y garantía de sus derechos» (Memorándum de Montevideo).

Las medidas especiales para la protección de los derechos de privacidad y datos personales de los menores exigen condiciones relacionadas con la concienciación, educación, control y supervisión que aseguren prácticas responsables de internet y redes sociales. En todo caso, frente al *sharenting*, lo que se intenta resaltar es la importancia de garantizar la identidad digital de los menores en la web:

> 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 han de 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 (Acedo y Platero, 2016: 74).

Estudios relacionados con la privacidad de los menores en la web revelan, por ejemplo, que «en Estados Unidos, el 92% de los niños menores de dos años tienen algún tipo de presencia en las redes sociales» (Otero, 2017: 412). Así también, según una encuesta aplicada por la firma de seguridad AVG:

12. Sobre esta definición, la Corte Interamericana enfatiza que las Directrices de Riad (Directrices de las Naciones Unidas para la prevención de la delincuencia juvenil) han señalado que «la familia es la unidad central encargada de la integración social primaria del niño, los Gobiernos y la sociedad deben tratar de preservar la integridad de la familia, incluida la familia extensa. La sociedad tiene la obligación de ayudar a la familia a cuidar y proteger al niño y asegurar su bienestar físico y mental» (Opinión Consultiva 17/2002, p. 64).

> En diez países, entre ellos España, recoge que el 23% de los niños tiene presencia en línea incluso antes de nacer, porque sus padres publican imágenes de las ecografías durante el embarazo. El porcentaje se dispara rápidamente, hasta el punto de que el 81% está en internet antes de cumplir los seis meses. La cifra sigue aumentando en los primeros años de la infancia.[13]

En materia de protección de datos, las limitaciones que se derivan del ejercicio del derecho a la protección de datos necesariamente deben converger con las obligaciones que supone el ejercicio de la patria potestad de los padres, con el objeto de garantizar el cuidado, el desarrollo integral y, en suma, la defensa de los derechos y garantías de los hijos. Lógicamente, en esta tarea el apoyo de los Estados es fundamental. Como precisa la Corte Interamericana de Derechos Humanos:

> En principio, la familia debe proporcionar la mejor protección de los niños contra el abuso, el descuido y la explotación. Y el Estado se halla obligado no sólo a disponer y ejecutar directamente medidas de protección de los niños, sino también favorecer, de la manera más amplia, el desarrollo y la fortaleza del núcleo familiar (Opinión Consultiva 17/2002, p. 63).

Desde esta perspectiva, hay que resaltar el deber del Estado y la sociedad en general. No obstante, la familia cumple un papel trascendental en el aseguramiento de la protección de los datos personales de la niñez y adolescencia.[14] Por tanto, el deber de garantizar este derecho fundamental no solamente es exigible al Estado y la sociedad. Con frecuencia decimos que «la familia es la primera escuela» y, en consecuencia, la tutela de este derecho fundamental debe proveerse también en gran medida de prohibiciones y mecanismos de control parental. Al respecto, se advierte que en el caso de la niñez y la adolescencia, «se deberá considerar la prohibición de tratamiento de datos personales», mientras que en el caso de los adolescentes «se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara» (Memorándum de Montevideo).

Hoy es indudable que la aparición de tecnologías como internet y redes sociales representan un cambio de paradigma en la protección de los datos personales, de la intimidad y la privacidad de las personas. En el caso de la niñez y adolescencia, el *sharenting* plantea en la familia nuevas problemáticas y tensiones entre el uso de las tecnologías y la protección de la privacidad y datos personales de los menores.

Por ello, los padres y quienes forman parte del vínculo familiar tienen la obliga-

13. Pilar Ponce de León, «El 81% de los bebés tiene presencia en la red antes de cumplir los seis meses», Universitat Oberta de Catalunya, 13 de agosto de 2019, disponible en https://bit.ly/39s18bh.

14. En este sentido, destacamos un deber tripartito, ya que, como advierte la Corte Interamericana, «la adopción de medidas especiales para la protección del niño corresponde tanto al Estado como a la familia, la comunidad y la sociedad a la que aquél pertenece» (Opinión Consultiva 17/2002, p. 63).

ción de «conocer que existen riesgos en el hecho de compartir información sobre sus hijos en las redes sociales. Entre los daños que pueden suceder se encuentra el robo de identidad y que se compartan imágenes en sitios que fomentan la pedofilia» (Otero, 2017: 412). Así, como hemos señalado en otro momento, se advierte «la necesidad de estimar mecanismos de control y prevención precisados en un modelo de cultura digital, respecto a los riesgos que representan sufrir amenazas, intimidación, extorsión y discriminación como resultado de la sobrexposición de información personal en entornos digitales» (Ordóñez, 2018: 390).

Por otra parte, es imprescindible estimar que estas limitaciones y mecanismos de control para la protección de los datos de carácter personal en la niñez y adolescencia, respectivamente, deben enmarcarse en el principio de interés superior, lo cual supone «que el desarrollo de éste y el ejercicio pleno de sus derechos deben ser considerados como criterios rectores para la elaboración de normas y la aplicación de éstas en todos los órdenes relativos a la vida del niño» (Opinión Consultiva 17/2002, p. 63).[15] En este contexto, puede decirse que, sobre la base de este principio, «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» (Acedo y Platero, 2016: 65).

Las referencias citadas en torno a la invasión de la privacidad de los menores en la web y los riesgos a los que se exponen demandan de la familia garantías para el ejercicio pleno de sus derechos en todos los órdenes, incluido el de protección de su identidad digital. De esta manera, las limitaciones y mecanismos de control de la información personal de los menores deben priorizar «el interés superior de niñas, niños y adolescentes, guardando un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de esas herramientas que representan formas de ejercicio de sus derechos» (Memorándum de Montevideo). En este plano, la actividad del Estado es primordial a efecto de asegurar que la familia se constituya en un verdadero núcleo central de protección que, en atención al principio de interés superior, pondere «no sólo el requerimiento de medida especiales, sino también las características particulares de la situación en la que se hallan el niño» (Opinión Consultiva 17/2002, p. 62).

Tomando en cuenta el desarrollo de las tecnologías, parece necesario centrar nuestra atención en la primera escuela, aquélla en que se adquieren valores y normas

15. Al respecto, la Corte Interamericana agrega que «este principio regulador de la normativa de los derechos del niño se funda en la dignidad misma del ser humano, en las características propias de los niños, y en la necesidad de propiciar el desarrollo de éstos, con pleno aprovechamiento de sus potencialidades, así como en la naturaleza y alcances de la Convención sobre los Derechos del Niño» (Opinión Consultiva 17/2002, p. 61).

de comportamiento básicos y necesarios para desenvolverse en sociedad: la familia.[16] Bajo estas consideraciones, corresponde señalar cuáles son las obligaciones y el papel que cumple la familia frente a lo que hemos denominado el «deber de corresponsabilidad digital» para la protección de datos personales de los menores.

Puede decirse que el concepto de corresponsabilidad se origina de una obligación tripartita que tiene el Estado, la sociedad y la familia de cara al aseguramiento, reconocimiento y respeto material de los derechos fundamentales en la comunidad. Como señala la Corte Interamericana de Derechos Humanos:

> No hay que perder de vista las limitaciones existentes en diversas materias, como el acceso de los padres al menor. Algunas de estas medidas constituyen un peligro para las relaciones familiares. Debe existir un balance justo entre los intereses del individuo y los de la comunidad, así como entre los del menor y sus padres. La autoridad que se reconoce a la familia no implica que ésta pueda ejercer un control arbitrario sobre el niño, que pudiera acarrear daño para la salud y el desarrollo del menor (Opinión Consultiva 17/2002, p. 62).

Así, en la era digital, la corresponsabilidad u obligaciones que corresponden a la familia es fundamental, dado que internet y redes sociales suponen nuevos paradigmas en que los menores desarrollan su personalidad e identidad digital. Por tanto, se advierte que «la privacidad es un derecho de los niños, así como su identidad en línea, que, a medida que crezcan, la irán armando y, por lo tanto, debe ser definida por ellos y no por sus padres» (Otero, 2017: 412).

En este sentido, es urgente «educar y concientizar a la ciudadanía en temas de privacidad en la red […] es el usuario común quien debe comprender el riesgo que conllevan sus acciones hacia su privacidad y la de terceros» (Herrera Carpintero, 2016: 96). Por ello, hay que destacar la importancia de «abrir verdaderos espacios de diálogo, supervisión y control en la familia, de tal manera que esta libertad informática pueda encajar con el desarrollo integral de los niños, niñas y adolescentes» (Ordóñez, 2018: 393). En suma, «se debe aconsejar a las familias sobre estos temas, ya que los padres pueden no tomar en cuenta que, al utilizar las redes sociales, pueden afectar el bienestar de sus hijos» (Otero, 2017: 412).

Por ejemplo, la reconocida Agencia Española de Protección de Datos, respecto de la sobreexposición de datos personales en internet, recomienda, por un lado, reflexionar antes de publicar cualquier tipo de información personal o imágenes, así como evitar compartir datos considerados como sensibles o especialmente protegidos.[17]

16. En cualquier caso, aquel núcleo fundamental en el que deben promoverse derechos y obligaciones recíprocas.

17. Agencia Española de Protección de Datos, «Protección…». La AEPD llama oversharing a la «sobreexposición de información personal en internet, en particular en las redes sociales a través de los perfiles de los usuarios».

> Lo que queremos destacar es que el fenómeno del *oversharing* cobra, si cabe, más importancia cuando la información que se comparte está protagonizada por los menores, y es que si bien no cabe duda de la buena intención de los padres al compartir fotografías y vídeos —tiernos, graciosos, llamativos u originales— de sus hijos, la pregunta que debemos hacernos es: ¿vulnera esta actitud el derecho del menor a la intimidad, el honor y la propia imagen? (Davara Fernández, 2017: 23).

Una pregunta de difícil respuesta. No obstante, recordemos que «los niños poseen los derechos que corresponden a todos los seres humanos —menores y adultos— y tienen además derechos especiales derivados de su condición, a los que corresponden deberes específicos de la familia, la sociedad y el Estado» (Opinión Consultiva 17/2002, p. 60). Al abundar información sensible de menores en la web, consideramos que los riesgos a los que se exponen no deben pasar desapercibidos, ya que pueden afectar bienes jurídicos especialmente protegidos relacionados con el desarrollo de su personalidad, integridad, privacidad y la propia imagen. Por esta razón, es indispensable «promover la sensibilización y la comprensión de todos los agentes implicados acerca de los riesgos, normas, garantías y derechos relativos a la utilización de las redes sociales, haciendo hincapié en que las actividades dirigidas específicamente a los menores de edad» (Davara Fernández, 2017: 98).

Así, en la familia, entre los deberes específicos llamados a precautelar la seguridad, bienestar y desarrollo de los menores en la web se destacan, además:

- La prevención —sin dejar de lado un enfoque de políticas, normativo y judicial— para enfrentar los aspectos identificados como riesgosos de la sociedad de la información y conocimiento, en especial del internet y las redes sociales digitales, fundamentalmente por medio de la educación.
- Proveer información y fortalecer capacidades de los progenitores y personas responsables sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales (Memorándum de Montevideo).

Así, en esta parte se destacan la prevención a partir de la información y educación sobre los riegos que suponen compartir información personal de los menores, destacándose el papel que cumplen los padres y personas responsables de su cuidado. En este sentido, conviene destacar que «es sobre todo a través de la educación que gradualmente se supera la vulnerabilidad de los niños» (Opinión Consultiva 17/2002, p. 71). Por tanto, es esencial que los padres y quienes comparten el vínculo familiar fortalezcan sus capacidades «sobre el impacto de las imágenes subidas a internet, así como la conveniencia de hacer conscientes tanto a los menores como a los adultos de los derechos y deberes —de unos y de otros— respecto al uso de internet en general y de las redes sociales en particular» (Davara Fernández, 2017: 24).

Conclusiones

Redes sociales e internet representan un gran avance en los procesos de desarrollo de las sociedades modernas. No obstante, si bien los objetivos del desarrollo tecnológico se orientan a eliminar la brecha y analfabetismo digital, la falta de concienciación sobre los peligros que supone el acceso a medios informáticos constituye una de las principales problemáticas, sobre todo en lo concerniente al respeto del derecho a la protección de datos e intimidad informática.

En la actualidad, el respeto del derecho a la protección datos personales y privacidad de los menores en la red tiene especial importancia. En el caso de la niñez y la adolescencia, el instituto de garantía que comprende la protección de la información personal exige la adopción de mecanismos especiales de tutela en virtud del grado de vulnerabilidad del que pueden ser objeto. Debido a que la información personal revela aquellas características propias de un individuo, las cuales pertenecen a la esfera de lo privado o íntimo, en entornos digitales la protección de la identidad de los menores es fundamental frente a los riesgos a los que pueden verse expuestos.

En general, la sobreexposición de información puede desencadenar en la revelación de los aspectos más íntimos de la persona. Genera, a su vez, una identidad digital, cuyo control pertenece únicamente al titular de la información. No obstante, en el caso de los menores, la construcción de la identidad digital parece, sin duda, corresponder a terceros (familiares y quienes ejercen la representación legal), quienes sin saberlo amenazan su privacidad y desarrollo integral.

La experiencia internacional en materia de protección de datos personales de niños, niñas y adolescentes ha motivado la adopción de una serie de instrumentos jurídicos (reglamentos, directrices, acuerdos) que comprometen en los Estados y la sociedad la adopción de leyes y políticas públicas orientadas a salvaguardas la integridad de los menores en la red. Sin embargo, como queda evidenciado en este estudio, muchos casos de sobreexposición de información personal provienen desde la misma familia (*sharenting*), por lo que resulta esencial plantear desde el núcleo familiar un modelo de cultura de protección de la información personal en entornos digitales.

La educación digital familiar y el fortalecimiento de destrezas y competencias digitales de los progenitores y representantes de los menores debe converger con el aseguramiento y plena satisfacción del principio de interés superior de los menores. Solamente garantizando un equilibrio entre deberes y derechos en la sociedad de la información podremos estimar que el tratamiento de la información de los menores cumple con el deber de corresponsabilidad a la que están sujetos el Estado, la sociedad y la familia.

Reconocimiento

Este artículo se deriva y es una ampliación de un apartado del trabajo de titulación de uno de los autores, Stefany Xiomara Calva Jiménez, en el marco de las estrategias académicas y adoptadas por la carrera de Derecho.

Referencias

Acedo, Ángel y Platero Alejandro (2016). «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». *Revista Chilena de Derecho y Tecnología*, 5 (2): 63-94. DOI: 10.5354/0719-2584.2016.42557.

Alarcón, José (2015). «El tratamiento del delito de pornografía infantil en la legislación ecuatoriana». Repositorio Institucional UASB-DIGITAL. Disponible en https://bit.ly/2UYtHUX.

Azurmendi, Ana (2018). «Derechos digitales de los menores y datos masivos: Reglamento europeo de protección de datos de 2016 y la COPPA de Estados Unidos». *Revista internacional de Información y Comunicación*, 27 (1): 27-35. DOI: 10.3145/epi.2018.ene.03.

Calva, Stefany (2020). «Protección de datos de carácter personal en la niñez y la adolescencia en internet: Riesgos y mecanismos de protección». Tesis para postular al grado de abogado, Universidad Técnica Particular de Loja, Ecuador. Disponible en https://bit.ly/3nNaHpb.

Castro, Alejandro (2013). «Formar para la ciberconvivencia: Internet y prevención del *ciberbullying*». *Revista Integra Educativa* 6 (2): 49-70. Disponible en https://bit.ly/3640YHT.

Conde, Concepción (2005). *La protección de datos personales: Un derecho autónomo con base a los conceptos de intimidad y privacidad*. Madrid: Dykinson.

Davara Fernández, Laura (2017). *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos. Breve referencia al fenómeno Pokémon Go*. Madrid: Boletín Oficial del Estado.

Eberlin, Fernando (2017). «Sharenting, liberdade de expressão e privacidade de crianças no ambiente digital: O papel dos provedores de aplicação no cenário jurídico brasileiro». *Revista Brasileira de Políticas Públicas*, 7 (3): 255-273. DOI: 10.5102/rbpp.v7i3.4821.

Fernández Sousa, Lucía (2015). «El delito de *online child grooming*». Trabajo final de máster en Abogacía, Universidad de Oviedo, España. Disponible en https://bit.ly/39bny09.

García-Atance, María (2017). «Diversas manifestaciones de riesgo social y moral del menor en el ámbito de técnicas de información y comunicación». *Revista de Derecho Político*, 100: 1.271-1.308. Disponible en https://bit.ly/3nNJcM2.

Gil, Ana (2013). *El derecho a la propia imagen del menor en internet*. Madrid: Dykinson.

Herrera Carpintero, Paloma (2016). «El derecho a la vida privada y las redes sociales en Chile». *Revista Chilena de Derecho y Tecnología*, 5 (1): 87-112. DOI: 10.5354/0719-2584.2016.41268.

Hidalgo, Alberto (2016). «Protección de datos de carácter personal relativos a la salud del paciente: Fundamentos, protección a la intimidad y comentarios al nuevo reglamento UE 2016/679». *Revista de Derecho UNED*, 19: 715-744. DOI: 10.5944/rduned.19.2016.18462.

Lathrop, Fabiola (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. DOI: 10.4067/S0718-34372013000300007.

Millán, Francisco y Juan Peralta (1995) «El derecho de autodeterminación informativa como derecho de la personalidad o derecho fundamental». Cuadernos de Estudios Empresariales, 5: 203-222. Disponible en https://bit.ly/3653Kd2.

Montesinos, Alejandro (2012). «La sociedad de la información y el gobierno electrónico». *Revista Chilena de Derecho y Tecnología*, 1 (1): 171-219. DOI 10.5354/0719-2584.2012.24029.

Ordóñez, Luis (2018). «Protección de datos personales: Precisiones para una cultura digital basada en la corresponsabilidad». En Luis Mañas, Sendy Meléndez y Rodrigo Estrella (compiladores), *La comunicación ante el ciudadano*. Barcelona: Gedisa.

Otero, Paula (2017). «*Sharenting*… ¿La vida de los niños debe ser compartida en las redes sociales?». *Archivos Argentinos de Pediatría*, 115 (5): 412-413. DOI: 10.5546/aap.2017.412.

Rebollo, Lucrecio y Carlos Saltor (2013). *Derecho a la protección de datos en España y Argentina*. Madrid: Dykinson.

Serrano, María y Lucrecio Rebollo (2008). *Introducción a la protección de datos.* Madrid: Dykinson.

Solé, Judith (2015). «La protección de los derechos al honor, a la intimidad personal y familiar y a la propia imagen de los menores y discapacitados». En Antoni Fayos Gardó (coordinador), *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Madrid: Dykinson.

Steinberg, Stacey (2017) «Sharenting: Children's privacy in the age of social media». UF Law Scholarship Repository. Disponible en https://bit.ly/3nWj3uE.

Troncoso, Antonio (2010). *La protección de datos personales: En busca del equilibrio*. Valencia: Tirant lo Blanch.

Sobre los autores

Luis Ordóñez Pineda es abogado. Especialista en derecho procesal penal por la Universidad Técnica Particular de Loja, Ecuador. Maestro en Derecho por la Universidad Nacional Autónoma de México. Candidato a doctor en Ciencias Sociales y Jurídicas en la Universidad de Cádiz, España. Profesor de Derecho Informático del Departamento de Ciencias Jurídicas de la Universidad Técnica Particular de Loja. Su correo electrónico es loordonez@utpl.edu.ec. https://orcid.org/0000-0002-0262-2212.

Stefany Calva Jiménez es abogada. Graduada en la Universidad Técnica Particular de Loja, Ecuador. Tesista en pregrado bajo la dirección del Mgtr. Luis Ordóñez Pineda con el tema «Protección de datos de carácter personal en la niñez y la adolescencia en internet: Riesgos y mecanismos de protección». Su correo electrónico es sxcalva@utpl.edu.ec. https://orcid.org/0000-0003-2269-7905.

REVISTA CHILENA DE DERECHO Y TECNOLOGÍA

La *Revista de Chilena de Derecho y Tecnología* es una publicación académica semestral del Centro de Estudios en Derecho Informático de la Facultad de Derecho de la Universidad de Chile, que tiene por objeto difundir en la comunidad jurídica los elementos necesarios para analizar y comprender los alcances y efectos que el desarrollo tecnológico y cultural han producido en la sociedad, especialmente su impacto en la ciencia jurídica.

EDITOR GENERAL
Daniel Álvarez Valenzuela
(dalvarez@derecho.uchile.cl)

SITIO WEB
rchdt.uchile.cl

CORREO ELECTRÓNICO
rchdt@derecho.uchile.cl

La edición de textos, el diseño editorial
y la conversión a formatos electrónicos de este artículo
estuvieron a cargo de Tipográfica
(www.tipografica.io).