

La privacidad y protección de datos de los menores de edad en la era de la tecnología disruptiva: El derecho al olvido, el *sharenting* y el *oversharenting*

The privacy and data protection of minors in the era of disruptive technology: The right to be forgotten, sharenting and oversharenting

Maryori Molina Luna 

Pontificia Universidad Católica de Valparaíso, Chile

RESUMEN

En la era digital, el derecho al olvido, el *sharenting* y el *oversharenting* son conceptos importantes relacionados con la protección de la privacidad y los datos personales de los menores de edad. Este artículo aborda la vulnerabilidad de este grupo ante la sobreexposición de información personal y sensible por parte de sus padres, cuidadores o terceros, la que puede afectar su dignidad, reputación y privacidad en el presente y en el futuro. Para ello, se establece un enfoque metodológico que incluye la revisión de la literatura sobre el *sharenting*, el *oversharenting*, el derecho al olvido y los derechos de privacidad y protección de datos de los menores en internet. Además, se plantean ejemplos que ilustran los desafíos existentes en este escenario. El resultado principal de esta investigación manifiesta la problemática de la protección de los menores debido a la sobreexposición de su imagen e información personal en el ciberespacio. En este sentido, se destaca el derecho al olvido como una facultad de control de la información personal, asumiéndolo como un instrumento del derecho a la protección de datos personales y como un mecanismo paliativo de tensiones entre padres e hijos.

PALABRAS CLAVE

Derecho al olvido • protección de datos • menores de edad • privacidad • *sharenting* • *oversharenting*

ABSTRACT

In the digital age, the right to be forgotten, sharenting, and oversharenting are important concepts related to the protection of the privacy and personal data of minors. This article addresses the vulnerability of this group to the overexposure of personal and sensitive information by their parents, caregivers,

or third parties, which can affect their dignity, reputation, and privacy now and in the future. To this end, a methodological approach is established that includes a review of the literature on sharenting, oversharenting, the right to be forgotten, and the privacy and data protection rights of minors online. In addition, examples are presented that illustrate the challenges in this context. The main result of this research highlights the problem of protecting minors due to the overexposure of their image and personal information in cyberspace. In this sense, the right to be forgotten is highlighted as a right to control personal information, assuming it as an instrument of the right to personal data protection and as a mechanism to alleviate tensions between parents and children.

KEYWORDS

Right to be forgotten • personal data protection • minors • privacy • sharenting • oversharenting

I. INTRODUCCIÓN

La actual omnipresencia de internet hace imprescindible —para enfrentar las diversas vulneraciones generadas por la tecnología digital— la existencia de garantías que reflejen valores fundamentales como la justicia, la equidad y la dignidad humana. En el ciberespacio, grupos como los menores de edad requieren protección adicional basada en normativas legales, morales y éticas, que sirvan como mecanismos preventivos de salvaguarda ante eventuales transgresiones en el espacio digital.

La protección de los datos personales es crucial pues puede prevenir vulneraciones o disminuir su impacto. Según el Reglamento General de Protección de Datos de la Unión Europea (RGPD)¹ existen dos categorías de datos que determinan los niveles de protección requeridos. En pri-

¹ Reglamento (Unión Europea) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Para este trabajo se considera que, de momento, el RGPD es la normativa más influyente a nivel mundial en materia de protección de datos. Las motivaciones de esta consideración obedecen a estos criterios: a) establece un marco sólido para la protección de la privacidad y los datos personales dentro de la Unión Europea y el espacio económico europeo; b) permite, aunque no sea del todo sencillo, dar marcha atrás al *sharenting* y cuidar con prudencia la identidad digital; c) el ámbito de aplicación extraterritorial del reglamento obliga a cualquier empresa u organización, dentro o fuera de la Unión Europea, que procese datos personales de residentes de este espacio, a cumplir con los parámetros legales contemplados en el mismo; d) esta normativa establece parámetros y obligaciones estrictas sobre cómo deben recopilarse, almacenarse y tratarse los datos personales; e) el impacto, incidencia e influencia que ha tenido en otras partes del mundo; f) académicos como Moritz Hennemann, Matthias Orthwein y otros, consideran que el RGPD es un referente de alto estándar en materia de privacidad y protección de datos, apreciación que es compartida por la autora de este artículo.

mer lugar, las categorías generales, que responden a los datos que pueden identificar directa o indirectamente a una persona: nombres y apellidos, número de teléfono, dirección, correo electrónico, identificadores en línea, entre otros. En segundo lugar, las categorías especialmente protegidas, que son los datos sensibles que requieren medidas de protección más estrictas debido a su potencialidad de discriminación o afectación: origen racial o étnico; convicciones y opiniones políticas, filosóficas o religiosas; afiliación sindical; datos genéticos, heredados o adquiridos, y biométricos (físicos, fisiológicos o conductuales); salud física, mental o emocional; orientación sexual, etcétera. Además, los datos inherentes a las condenas o infracciones penales requieren un nivel elevado de protección y están sujetos a un régimen particular, determinado por el tipo de delito, pena y otros factores del sistema penal nacional correspondiente.

De modo que, para este trabajo, los datos especialmente protegidos de los menores son los que se circunscriben a ese estricto ámbito de protección al cual se hace referencia. Históricamente, se ha delegado en los padres o tutores legales, y en términos amplios, en el Estado, la responsabilidad de proteger los derechos de los niños. Con el auge de la tecnología digital, han sobrevenido nuevos riesgos de vulneración, dentro de los cuales el *sharenting* y el *oversharenting* tienen un lugar preponderante. El primer concepto se usa para identificar la tendencia, cada vez mayor, de algunos padres, representantes legales o terceros a compartir a través de plataformas digitales —con o sin intención— información personal y especialmente sensible de sus hijos o menores de edad sin su consentimiento. El problema potencial de esta tendencia es que, en la medida que los niños crecen y maduran, pueden disentir con la forma en que su información personal ha sido o es compartida por sus padres, tutores o terceros cuidadores. Se trata, con todo, de un problema reciente para cuya comprensión es necesario echar una mirada a los cambios generacionales y su relación con la tecnología de la internet.

Generacionalmente, el impacto de la internet ha sido diverso. A los *baby boomers* (nacidos entre 1946 y 1964) y a la generación X (nacidos entre 1965 y 1981) el internet les ha sorprendido, mientras que a los *millennials* (nacidos entre 1982 y 1999) internet les ha pasado por encima². Esta

² La cuestión generacional es de importante consideración a propósito del problema que trata este artículo. La generación X y los *millennials* debieron gestionar el fenómeno del internet de forma intuitiva y, por lo mismo, no lograron advertir a tiempo las profundas transformaciones que la era digital suponía para las viejas prácticas sociales. Siguieron sacando las mismas fotografías de sus hijos y mantuvieron los mismos deseos de compartirlas; pero no dimensionaron la diferencia que media entre el álbum familiar guardado

última generación se fue adaptando a medida que la tecnología avanzaba y, a diferencia de las anteriores, la mayoría de los *millennials* tienen vagos recuerdos de lo que era un mundo sin internet, o al menos, vivieron su adolescencia en plena masificación de la era digital. Pero, las generaciones más recientes, es decir, los *centennials* (nacidos entre 1997 y 2012) y la generación alfa (nacidos entre 2013 y la actualidad) están inmersos en la era digital desde su nacimiento. En palabras de Boyd, son parte de la primera generación nacida propiamente en la era digital y sus padres son los primeros en educar enteramente a «niños digitales»³.

Cada vez es más habitual que la huella digital de un niño comience antes de su nacimiento, con ecografías o ultrasonidos —fotos o videos— captadas en el útero de la madre y que son compartidas por los padres u otros familiares en las plataformas digitales. Siguiendo los datos ofrecidos en el documento —avalado por la Organización de las Naciones Unidas— del Organismo Nacional de Protección de Datos y Libertad de Información de Hungría, «el 80 % de los niños que viven en los países occidentales desarrollados tienen una huella digital antes de los 2 años»⁴.

Esta exposición temprana generalmente se lleva a cabo sin el consentimiento expreso de las personas y se une a la masificación y tratamiento de datos que alimenta un modelo de economía que monetiza la información. Esto representa un peligro enorme para los derechos digitales de todos, pero especialmente para los menores. Particularmente, estos siempre serán más vulnerables, sobre todo cuando se trata de los riesgos de internet: ciberacoso; *phishing*; *grooming*; *sexting*; *bot baby*; exposición a contenido inadecuado; robo o suplantación de identidad; etcétera. Por ello, la protección de su privacidad es fundamental para mitigar estos y muchos otros peligros. Pero, ¿qué ocurre cuando son los propios padres, tutores legales o terceros cuidadores quienes exponen en el espacio digital la imagen del menor y con esto han comprometido su privacidad? En esos casos, al igual que con los adultos, deberían existir medidas destinadas a enmendar las lesiones ocasionadas.

Así, aparece y se fundamenta el derecho al olvido digital como una de las facultades jurídicas actuales que, aun siendo perfectible, otorga a las personas —al menos a los residentes en la Unión Europea—, bajo determinados supuestos, la posibilidad de solicitar la supresión o desvin-

en la intimidad del hogar y la plataforma digital y pública en la que sus hijos constituyen un dato del sistema y conforman su rastro digital de por vida.

³ BOYD (2011), pp. 39-59.

⁴ Organización de las Naciones Unidas, Asamblea General, 22 de febrero de 2021, resolución A/HRC/46/37.

culación de información personal que vulnera sus derechos a la privacidad y a la protección de datos y que, además, impide la posibilidad de una segunda oportunidad o de tener una vida en la que acciones o información contenida en la web afecte su presente o su futuro. En esa dirección, este artículo reflexiona sobre el *sharenting*, el *oversharenting* y las implicaciones que estos fenómenos generan en el resguardo de la privacidad y la protección de los datos personales de los menores. También analiza cómo el derecho al olvido puede considerarse una importante facultad de protección en ese escenario.

II. EL *SHARENTING* Y LA PRIVACIDAD VIRTUAL DE LOS MENORES DE EDAD

La llegada al mundo de un nuevo bebé, su primera comida sólida, su primer gateo, sus primeros pasos, sus primeras palabras, el primer día de colegio, el acto de grado escolar, su primera licencia, son solo algunos hitos relevantes en la vida de un menor y, casi siempre, son motivos de orgullo y celebración para sus padres, quienes buscan capturar el momento con fotos o videos que, muy posiblemente, compartirán con familiares y amigos a través de las plataformas digitales de su preferencia. Pero, los niños o adolescentes no siempre disfrutan o están conscientes de la forma en que esos espacios de su vida son expuestos por sus padres en el espacio digital.

Según datos del Consejo de Derechos Humanos de la Organización de las Naciones Unidas⁵, más de una cuarta parte de los niños de diez, once y doce años que en 2017 fueron parte de una encuesta, manifestaron sentirse avergonzados, ansiosos y preocupados a raíz de las publicaciones en línea que su padres hacían de ellos. También, dos de cada cinco indicaban su incomodidad cuando amigos, familiares u otros publicaban alguna información sobre ellos sin tener previamente su permiso para hacerlo. Esto pone de manifiesto una situación crucial: la importancia del consentimiento. Muchas veces se da por sentado que las demás personas no tienen inconvenientes para publicar su imagen en medios digitales. ¿Qué podría pasar con una simple e inocente publicación? La realidad es que pueden existir infinitas razones que expliquen por qué se prefiere resguardar la privacidad o proteger los datos personales. Solicitar el consentimiento a otra persona antes de publicar algo sobre ella debería ser un principio mínimo requerido por costumbre social. No obstante, esto no siempre ocurre, sobre todo cuando se trata de menores de edad.

⁵ Organización de las Naciones Unidas, Asamblea General, 22 de febrero de 2021, resolución A/HRC/46/37.

En promedio, cada año un niño aparece, aproximadamente, en 195 fotografías compartidas sin su consentimiento⁶. De mantenerse ese ritmo de publicación, para su quinto cumpleaños tendría un portafolio equivalente a unas mil fotografías aproximadamente. Además, se estima que cerca de un 80% de los niños tiene una huella digital construida antes de sus dos años⁷. Esta práctica parental es conocida como *sharenting* y constituye, actualmente, un importante desafío jurídico a resolver, pues en el entono digital existe un compromiso y vulnerabilidad evidente de derechos personales de los menores de edad, especialmente, los derechos de privacidad y de protección de datos.

1. *Comprendiendo el sharenting*

Sharenting es un acrónimo anglófono de los términos *sharing* (compartir) y *parenting* (paternidad o parentalidad). El origen puntual es difícil de determinar, pues surgió de forma natural junto al crecimiento de las plataformas digitales y la tendencia de los padres de publicar aspectos personales y privados de sus hijos en estas redes. Así, en la medida en que las redes sociales pasaron a ocupar un lugar preponderante en la rutina de las personas, sobre todo en la primera década del siglo XXI, esta práctica empezó a ser más sobresaliente y a convertirse en un fenómeno creciente de «difusión en redes sociales de imágenes y comentarios sobre los hijos, menores de edad, por sus padres o madres o por ambos simultáneamente»⁸. Esto se vio incrementado durante la pandemia de covid-19, sobre todo durante los meses de confinamiento⁹.

El documento de South Australian Commissioner for Children and Young People establece que el *sharenting* es una tendencia en que los padres o futuros padres comparten en internet, de forma pública o restringida, información personal o sensible de sus hijos, lo que conforma una identidad en línea mucho antes de que este tenga capacidad para dar su consentimiento o comience a crear su propia huella digital¹⁰. Respecto de este tema, Verswijvel y Ouvrein¹¹ indican que son diversas las motivaciones que lo explican. Por un lado, se encuentra el deseo de compartir con la propia familia, elaborando álbumes de fotografías y videos familiares. Pero, por otro lado, también destacan las razones relacionadas con

⁶ KLUCAROVA Y HASFORD (2021), p. 2.

⁷ SOUTH AUSTRALIA COMMISSIONER FOR CHILDREN AND YOUNG PEOPLE (2020), p. 3.

⁸ KOPECKY *et al.* (2021), p. 1.

⁹ MUHAMMAD *et al.* (2020).

¹⁰ SOUTH AUSTRALIA COMMISSIONER FOR CHILDREN AND YOUNG PEOPLE (2020), p. 3.

¹¹ VERSWIJVEL Y OUVREIN (2019), p. 322.

la imagen que se proyecta en las redes sociales, por ejemplo, para ser vistos como buenos padres. También, puede ser por motivos colaborativos, como cuando se requieren donativos por temas de salud o discapacidades.

Por su parte, Steinberg afirma que la información que los padres comparten en línea sobre sus hijos puede ser potencialmente peligrosa, ya sea de forma intencional o no¹². Este escenario incide directamente en la creación de espacios de vulnerabilidad de derechos fundamentales: a la identidad, imagen e intimidad, pues cualquier persona en el mundo con acceso a internet podría acceder a la información publicada y usarla con una infinidad de intenciones. Esto es especialmente importante si esta práctica tiene un objetivo eminentemente económico. Retomando a Verswijvel y Ouvrein, cuando existen motivos de monetización se entra en el *sharenting* lucrativo, entendido como la práctica deliberada de compartir información de los hijos en plataformas digitales con la finalidad de conseguir beneficios económicos¹³. Acá pueden considerarse los patrocinios; la publicidad y promoción de productos, servicios o marcas; o la generación de contenido donde los hijos son protagonistas y con ello se generan formas de lucro en línea. Además, estas publicaciones —que contienen información personal del menor— suelen hacerse en modo público, permitiendo el acceso indiscriminado a las imágenes y comentarios sobre el niño, tal como sucede con los padres creadores de *blogs* o administradores de cuentas en plataformas digitales, cuyo objetivo va más allá del simple hecho de compartir; lo que exacerba la vulnerabilidad de los menores en internet.

2. Riesgos del sharenting

Los peligros asociados a la exposición de la imagen de los menores de edad en internet son infinitos, incluso, en estos momentos no somos conscientes de muchos de esos riesgos. Es importante precisar que esta exposición no solo afecta los derechos a la privacidad y a la protección de datos, sino que también trastoca otros derechos conexos, como la autodeterminación informativa; la intimidad familiar; la identidad digital; la integridad personal; y la libertad de expresión; entre otros. No obstante, ya existe suficiente evidencia de las terribles consecuencias que este fenómeno está trayendo consigo. Dan cuenta de ello delitos como la pornografía infantil; explotación sexual; trata de personas; el *ciberbullying*; el ciberacoso; *grooming*; sextorsión; la suplantación o robo de identidad; fraude digital; el *deepfake*; difamación y daños a la reputación; violación de derechos de autor.

¹² STEINBERG (2017), p. 843.

¹³ VERSWIJVEL Y OUVREIN (2019), p. 323.

Es importante considerar que, para los padres, tomar fotos o grabar videos de momentos especiales que desean atesorar es, en muchos casos, una muestra de amor y orgullo. Pero también esas *evidencias de amor* pueden ser relativas y subjetivas, y lo que para los padres puede ser una demostración de afecto, puede significar un bochorno, una vergüenza o un momento incómodo para los hijos. Con la invención de los primeros dispositivos tecnológicos que permitieron capturar imágenes, ha existido un deseo constante de inmortalizar momentos. Sin embargo, la diferencia entre el pasado y el presente radica en el ámbito, alcance y perduración de esas imágenes, audios, videos o incluso información personal. Antes, la vergüenza o la incomodidad se limitaban al salón de casa mientras familiares o cercanos veían fotos que, probablemente, preferiríamos mantener en privado. En estos momentos, esta realidad se ha trasladado al entorno digital, donde los recuerdos, comentarios y, en general, la información personal pueden ser vistos, guardados y usados por una cantidad indeterminada de personas en el mundo entero. Todo lo que se comparte en internet, en esencia, permanece allí. Aun cuando se asume que se ha eliminado una información puntual, como una imagen, video o comentario, esta seguirá estando disponible por otras vías: capturas de pantalla; descargas realizadas por terceros; almacenamiento en nubes vinculadas a plataformas digitales —OneDrive, Dropbox, Google Drive, Amazon Drive, Apple iCloud, Box, Mega, etcétera—; almacenamientos en red (Nas); datos compartidos o tratados; la *deep web*; entre otros medios. En realidad, no se tiene plena consciencia de la extensión de la distribución o ubicación de la información personal en el ilimitado ciberespacio.

Mientras los niños no son conscientes del significado e importancia de conceptos como reputación, privacidad o protección de datos, es posible que no perciban las implicaciones de que su información personal sea compartida en línea. Sin embargo, en la medida que estos niños crecen y se convierten en adolescentes, y luego en adultos, adquieren el discernimiento propio de la madurez y comprenden que parte importante de su autonomía radica en el control de su información personal y la forma en que desean que se conforme su rastro digital.

Justo en este punto, los menores que han estado expuestos —sin su consentimiento— a altos niveles de *sharenting* y que han asimilado las consecuencias de esta realidad, entienden los riesgos a los que están o han estado sometidos. La infinidad de datos y metadatos que han constituido su huella digital desde su nacimiento, e incluso desde antes de nacer, han alimentado su perfil predictivo digital y, a su vez, han coadyuvado en la generación de estrategias monetizables, por ejemplo, el *retargeting*. Este,

aunque es una herramienta efectiva del marketing digital, no deja de representar un peligro para la autonomía y el libre discernimiento de las personas. Además, otras situaciones, como la creación de perfiles invasivos o discriminatorios; la cibervigilancia; los riesgos de seguridad cibernética, y otras más, son situaciones que evidencian los altos niveles de vulnerabilidad que existen en el espacio digital, sobre todo, para los niños.

3. *Del sharenting monetizado al oversharenting*

En 1991, la emblemática banda de rock, Nirvana, lanzó su álbum *Nevermind*. En la portada se muestra la fotografía de un bebé desnudo —capturada por el fotógrafo Kirk Weddle— sumergido en una piscina y tratando de atrapar un dólar estadounidense atado a un anzuelo. Esta pasó a ser una imagen icónica, reconocida en el mundo entero y, además, se convirtió en un símbolo de juventud y rebeldía. Treinta años después, el 24 de agosto de 2021, Spencer Elden, el bebé protagonista de dicha portada, interpuso una demanda en contra de la banda, del fotógrafo y de Courtney Love (viuda y heredera de Kurt Cobain)¹⁴. Con dicha demanda, el bebé *Nevermind* tuvo la pretensión de exigir una indemnización a propósito de los daños que, según alegó, ha sufrido y sufrirá por el resto de su vida pues su imagen se utilizó como pornografía infantil y con intenciones netamente comerciales¹⁵.

Por otro lado, está el caso de Rohee Jinmiran o Jinmiran baby, una niña surcoreana de cuatro años que en 2019 se hizo famosa, o viral en términos actuales, por ser la imagen de innumerables memes, stickers y gifts. La niña se *viralizó* luego de que su progenitora compartiera en su cuenta personal de Instagram —aunque pública— fotografías de ella junto a su hermana, destacando sus gestos y reacciones. La madre no imaginó el alcance que tendrían dichas fotografías, ni que la cuenta llegaría a tener cerca de 1.5 millones de seguidores. Mucho menos intuyó que la imagen de su hija sería objeto de ese tratamiento en las plataformas digitales. En ese contexto, la madre de Jinmiran baby posteó en su cuenta de Instagram un comunicado en el que exige, puntualmente, que no se copien ni se capturen fotos de su hija, sin la debida autorización, para ser usadas con fines

¹⁴ United States, District Court II Central California, 24 de agosto de 2021, cv-06836.

¹⁵ El tribunal, con exposición del juez Fernando Olguin, desestimó la demanda fundamentando que, entre otras razones, el plazo de reclamo prescribió en 2011. No obstante, sin perjuicio de lo anterior, hubo importantes cuestionamientos sobre la fotografía, y si esta constituía o no material de explotación sexual infantil. Particularmente, resaltan en la sentencia las argumentaciones sobre los derechos a la privacidad y protección de datos de los menores de edad y el rol que ejercen en ello los padres.

publicitarios o como forma de comunicación visual entre plataformas digitales. Pero esto no obedece al resguardo de la privacidad o protección de datos de la niña en el presente o en el futuro, sino que responde a motivos comerciales, pues la menor ha firmado varios contratos publicitarios en los que se exige la protección de su imagen.

Otro caso que va en la misma dirección ocurrió en Turquía, donde en 2020 un hombre interpuso una demanda de divorcio alegando que su cónyuge exponía a abusos a sus hijos por compartir información audiovisual de ellos en plataformas digitales y por hacerlos aparecer en programas de televisión con el fin de convertirlos en celebridades¹⁶. También, en Francia, se han planteado causas judiciales de hijos en contra de sus padres por compartir contenido audiovisual en el que se exponía sin su consentimiento información personal de naturaleza sensible, lo que generó consecuencias no deseadas a largo plazo¹⁷.

Más allá de las opiniones personales que pueden generarse por estos u otros casos, y de los necesarios debates parentales, éticos, morales y jurídicos que deben darse al respecto, estos se exponen para visibilizar la complejidad existente en torno a la privacidad y a la protección de datos de los menores, en especial los de naturaleza sensible, en la realidad digital. Aunque estos casos corresponden a realidades, contextos y momentos históricos diferentes, reflejan una importante situación relacionada con la tecnología digital: la masificación de la información y los altos niveles de vulnerabilidad de la privacidad, especialmente la de los niños.

El *sharenting*, hasta cierto punto, sugiere intenciones inocentes, sobre todo si este se entiende como la práctica llevada a cabo por los padres, cuidadores o terceros, que consiste en publicar información de sus hijos solo por el deseo de compartir instantes vividos en familia, o para solicitar algún tipo de ayuda —no monetaria— por medio de la actividad en línea. De modo que, aunque la exposición de información personal de menores siempre será tema de discusión, esto puede ser tolerado hasta cierto punto y siempre que sean respetados los derechos de los niños. En este sentido es importante considerar que puede que no todo esté mal con el *sharenting*, aunque por razones lógicas esto admita discusiones válidas y muy pertinentes en contra. Pero, siempre que existan límites, criterios equilibrados y responsables en la exposición de la información, y que no se obtenga ningún tipo de beneficio por esta práctica, podría decirse que es una forma eficiente de mantener contacto con la familia, con personas

¹⁶ AYTEN *et al.* (2021), p. 13.

¹⁷ AYTEN *et al.* (2021), p. 13.

especiales o del entorno de confianza. También, es una manera de empatizar, buscar apoyo o validación ante determinadas circunstancias propias de la crianza; o una forma en la que se puede documentar el crecimiento o desarrollo de uno o varios niños, tal como sucede con algunos centros educativos, deportivos, artísticos, etcétera, que ven en la tecnología digital una aliada para demostrar el talento, modelos educativos, técnicas de enseñanza, entre otros temas. No se pretende establecer de forma inequívoca que sea así; al contrario, esto requiere importantes reflexiones, decisiones, acciones y protecciones.

Ahora bien, en el escenario contrario, las alarmas se encienden cuando las intenciones del *sharenting* dejan de ser enteramente personales o familiares y prevalecen intereses económicos. En ese caso pasa, a considerarse como monetizado o lucrativo, una variante en que los padres exponen la imagen de su hijo en internet con el fin de obtener beneficios económicos como publicidad, patrocinios, intercambios, pagos por un determinado servicio, etcétera. Este escenario refleja la complejidad en torno a la protección jurídica, la ética y la moral que deben prevalecer en lo referente al bienestar de los menores involucrados. Además, existe una delgada línea entre el *sharenting* monetizado y el *oversharenting* que, de ser cruzada, tal como lo asume la Corte Constitucional de Colombia, afectaría la privacidad y la identidad digital de los menores¹⁸, así como otros derechos conexos.

Plunkett, por su parte, establece sobre el *commercial sharenting* (sobre exposición comercial) que describe la forma específica en la que los padres o representantes legales comparten en plataformas digitales información, fotos o historias sobre sus hijos o menores de edad bajo su cuidado o responsabilidad legal, con fines de lucro o con un beneficio económico. Esta información, *a posteriori*, puede ser usada por terceros con fines de marketing, monetización o cualquier forma de publicidad sin que exista el explícito consentimiento o comprensión de dicha situación por parte del menor. Además, existen infinitas posibilidades de que el contenido compartido sea recolectado por algoritmos de inteligencia artificial (IA) y utilizados para crear perfiles de marketing digital o publicidad dirigida o personalizada, lo cual puede invadir su privacidad e influir en su futuro, tanto digital como físico, sin su consentimiento informado¹⁹.

¹⁸ Corte Constitucional de Colombia, 1 de julio de 2022, sentencia T-245A.

¹⁹ PLUNKETT (2019), p. 83.

4. *Comprendiendo el oversharenting*

El origen etimológico del término *oversharenting* es impreciso o difuso, pero, tal como sucede con *sharenting*, puede considerarse en términos generales que su auge se dio en la primera década del siglo XXI con el vertiginoso avance de redes sociales como Facebook, Twitter, Instagram y de *blogs* personales. Este concepto, también es un acrónimo de origen anglófono que se da como resultado de la combinación del prefijo *over* (en exceso o demasiado) y el término *sharenting*. Por tanto, puede traducirse como sobreexposición y definirse como la acción de compartir en exceso contenido sobre menores en internet, más allá de lo que sería considerado apropiado o seguro.

El *oversharenting* tiene una connotación negativa, pues lleva implícita la sobreexposición de los menores en internet lo que puede tener consecuencias negativas para su privacidad y seguridad. Esa sobreexposición crea la identidad digital del menor y suele darse sin su consentimiento explícito. La información compartida puede contener detalles íntimos, personales o de contenido sensible que, a futuro, afecten su vida personal y laboral. Además, puede tener efectos negativos en el desarrollo psicológico y social de los menores, lesionando su autoestima y su visión lógica de la privacidad.

Esta realidad evidencia y plantea importantes retos y preocupaciones. Entre ellos, el de la privacidad de los menores en el espacio digital; la necesidad de delimitar las fronteras entre lo público y lo privado en la realidad virtual; el establecimiento de principios éticos corporativos en el diseño y desarrollo de modelos de IA; y en la formulación de normativas jurídicas que, por un lado, garanticen la protección de los derechos personales en el espacio digital y, al mismo tiempo, fomenten y propicien la invención y el desarrollo tecnológico responsable.

La Agencia Española de Protección de Datos (AEPD) establece una visión bastante general de lo que constituye el *oversharenting*. Sobre este, afirma que es una de las tendencias negativas de internet y lo define como «la sobreexposición de información personal en internet, en particular en la redes sociales a través de los perfiles de los usuarios»²⁰. Para Hall, es una forma de sobreexposición digital que realizan los padres en detrimento de sus hijos, para alcanzar o satisfacer objetivos meramente personales. En términos generales, la autora propone que los padres buscan, en alguna

²⁰ Agencia española de protección de datos (2020).

medida, conseguir validación e inclusión social por medio de la sobreexposición de sus hijos²¹.

Esto coincide con lo planteado por Klucarova y Hasford, quienes afirman que esta práctica evidencia que los padres que sobreexponen a sus hijos intentan ser el centro de atención a través de ellos, ser validados y reconocidos como buenos padres, o encajar en la realidad tecnológica digital que ha impuesto los *likes* como una forma de ser admirados por los demás²². Además, estos autores agregan que una de las principales razones por la que los usuarios de las redes sociales comparten información personal es para desarrollar una identidad que les permita afiliarse con otros. Lo cual no es extraño, pues la afiliación es una necesidad humana que, además, manifiesta el deseo de pertenecer y participar socialmente²³.

Esto necesariamente conduce a revisar la relación que existe entre el *oversharing*, el *sharenting* y el *oversharenting*. Parafraseando a Davara Fernández, el primero es una práctica donde las personas exteriorizan el gusto por lo social y por compartir todo tipo de información personal sin límite en redes sociales²⁴. El segundo, como hemos visto, consiste en la práctica de los padres de publicar en plataformas digitales contenido familiar centrado en sus hijos. Este puede incluir fotos, historias, videos o cualquier otra información relacionada con la vida de los menores. Esta modalidad, además, tiene una variante monetizada, que se realiza con fines eminentemente económicos. El *oversharenting*, por su parte, describe la práctica según la cual los padres publican de forma excesiva información sobre sus hijos en las redes sociales. Esta práctica excede al *sharenting* e implica la sobreexposición del menor y la afectación de su privacidad y otros derechos conexos. En tal sentido, en la medida que los padres o adultos cuidadores sobreexpongan contenido, pueden pasar a los otros dos campos, según como corresponda. Todo dependerá de la forma, intensidad y objetivos que persigue.

En ese contexto, Holzer entiende que «el *oversharing* es un fenómeno social todavía fuera del control de sus actores [que se realiza] sin entender o mostrar verdadera preocupación, en cuanto a las posibles consecuencias»²⁵. Esta nueva generación de padres son más asiduos a exponer su vida personal y familiar en redes sociales y, consecuentemente, con ello se exponen aspectos de la vida privada de sus hijos. Esto se complementa con

²¹ HALL (2018), p. 125.

²² KLUCAROVA Y HASFORD (2021), p. 2.

²³ KLUCAROVA Y HASFORD (2021), p. 3.

²⁴ DAVARA FERNÁNDEZ (2017), p. 23.

²⁵ HOLZER (2017), p. 103.

lo establecido por este autor, quien afirma que «el exceso que caracteriza a través del “*over*”, es una ilustración más de la sobremodernidad; sobreproducción de imágenes de sus hijos, generando sentido para sí mismo»²⁶. De este modo, pudiera ocurrir que como consecuencia de esta práctica de sobreexposición se afecte la identidad digital de los menores.

Dentro de este fenómeno, Haley realizó un estudio sobre el derecho al olvido y el *sharenting*. La autora sostiene que compartir demasiado en las plataformas digitales representa —inmediatamente y a largo plazo— un riesgo significativo para los derechos de los niños, cuando son los padres quienes la comparten. Según Haley, los niños son un objetivo particularmente vulnerable ante diversos delitos digitales. Además, para la autora, cuando los padres comparten información personal de sus hijos, como fecha de nacimiento, dirección particular, ubicación actual o frecuente, entre otros, los exponen en altos niveles a sufrir crímenes violentos como agresiones físicas, secuestros, o abusos sexuales, lo que es particularmente preocupante dado que el 76 % de los secuestros y el 90 % de los crímenes violentos contra menores son perpetrados por familiares o conocidos²⁷.

Ordóñez y Calva, en tanto, advierten que «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»²⁸. Azurmendi, coincidiendo con el criterio de Haley, Ordóñez y Calva, considera que el menor está en una evidente situación de desprotección, pues el adulto que le tutela, prevaliéndose de su ascendencia, vulnera su privacidad y otros derechos al vender, intercambiar o difundir sus datos. Agrega Azurmendi que estas situaciones podrían tomarse como faltas a las responsabilidades de la tutela legal del menor y, en consecuencia, deben preverse sanciones para este tipo de conductas abusivas²⁹.

Ahora bien, esto plantea un panorama mucho más complejo y controvertido, pues se traspasan los límites del interés y libertad de los padres en el cuidado, crianza, custodia y control de sus hijos. Aun cuando el *sharenting* y el *oversharenting*, en menor o mayor medida, constituyen evidencia de la extralimitación o ausencia de garantía de un genuino resguardo de la privacidad e identidad del menor por parte de los padres o los cuidadores legales; es claro que en este contexto tecnológico digital hay, por parte de

²⁶ HOLZER (2017), p. 96.

²⁷ HALEY (2020), p. 1007.

²⁸ ORDÓÑEZ Y CALVA (2020), p. 105.

²⁹ AZURMENDI (2018), pp. 27-35.

los padres, una tendencia creciente a utilizar internet con límites bastante difusos en lo que respecta a la publicación de información personal sobre sus hijos. Esto pone de manifiesto que, en la actualidad, hay significativos conflictos entre el deber de protección de la privacidad del niño y ciertos derechos de los padres o adultos cuidadores. Así, se observa que las libertades relacionadas con la expresión de los padres y el libre desenvolvimiento de la paternidad, respecto a la crianza de sus hijos, están en tensión. Este aspecto se abordará más adelante, justo después de comprender cuáles son las secuelas, peligros o consecuencias de *sharenting* y el *oversharenting*.

5. Consecuencias o riesgos

Los niños y adolescentes son particularmente vulnerables en todos los ámbitos de la vida debido a la etapa de desarrollo físico, cognitivo, psicológico y emocional en la que se encuentran. Así, suelen carecer del discernimiento necesario que les alerte sobre los peligros, sobre la necesidad de defenderse, o sobre la importancia de tomar decisiones informadas. Además, la falta de experiencia y comprensión de muchos aspectos de la realidad les hace más proclives de ser manipulados, explotados o dañados. Ahora bien, si a ese contexto se le adicionan los riesgos propios del entorno digital, aumentan en enormes proporciones las situaciones en las que los derechos de los niños pueden ser transgredidos.

Como se ha visto, que los padres compartan en internet demasiada información personal de sus hijos menores puede significar peligros o amenazas significativas, inmediatas y a largo plazo para estos. El *sharenting*, ya sea con fines personales o monetizado, y el *oversharenting* pueden exponer inadvertidamente detalles íntimos de la vida de los niños, como sus aficiones, gustos personales, tipo de comida favorita, ubicación, centro educativo en el que estudian, rutinas diarias, etcétera. Incluso si los padres limitan el acceso a sus publicaciones mediante controles parentales o filtros de privacidad en las plataformas digitales, aún existe el riesgo de que dicha información sea recolectada y guardada para luego ser usada o publicada en sitios *webs* no seguros o para generar publicidad personalizada.

Con la divulgación de esa información los menores quedan expuestos a personas malintencionadas, delincuentes o individuos con parafilias, que pueden emplear ese contenido para manipular, acosar, buscar la forma de entablar contacto directo, suplantar o robar la identidad, entre otros. Aunado a ello, cuando el niño tiene una huella digital desde temprana edad se genera el peligro de infringir —de innumerables formas— su privacidad e identidad, pudiendo llegar a afectar, en el presente y en el futuro, su reputación, su bienestar físico, psicológico y emocional y, en general,

muchos otros ámbitos de su vida. Al respecto, la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales establece que «*las niñas, niños y adolescentes están sujetos a una especial exposición y vulnerabilidad en los entornos digitales*»³⁰ y, por tanto, se les debe proveer de especial protección «*frente a prácticas abusivas, discriminatorias y violentas en los entornos digitales, así como frente a contenidos digitales que puedan resultar traumáticos o dañinos para su desarrollo integral o promover actitudes discriminatorias o vejatorias*»³¹.

En este sentido es posible afirmar que los padres pueden impactar negativamente la vida de sus hijos en varios aspectos. En primer lugar, está la transgresión a su privacidad: este es posiblemente el derecho que más se ve comprometido ante la exposición constante de información que debe ser especialmente protegida, no solo de manera inmediata, sino también a lo largo de toda la vida de la persona. Junto a este impacto, encontramos la identidad digital en peligro: cuando los padres han compartido en exceso detalles íntimos de la vida de sus hijos —rutinas, ubicaciones, afinidades, etcétera— los exponen tanto en el espacio virtual como en su vida cotidiana a ser presa fácil de la comisión de delitos como el ciberacoso; *grooming*, *phishing*; *sexting*; pornografía infantil; robo o suplantación de identidad; trata de personas.

Asimismo, puede ocurrir una afectación de la reputación digital: la permanencia indefinida de la información en bases de datos puede impactar la reputación digital de una persona no solo en el presente sino también en el futuro, afectando negativamente varios aspectos de su vida a largo plazo. Relacionado con esto ocurre una *pérdida de control de la información publicada*: el derecho de autodeterminación informativa adquiere especial relevancia en el contexto actual de internet, donde la accesibilidad, recopilación, descarga, almacenamiento y compartición masiva de información personal se hace con gran facilidad. Lo que se publica en internet se queda en internet, escapando la información del control del usuario. En ese espacio, se pierde la capacidad de gestionar la distribución, uso, almacenamiento e incluso, la eliminación de datos personales, lo que dificulta determinar quién tiene acceso a ellos y cómo se emplean. En este punto, utilizar como referencia el caso de Jinmiran baby da un valor añadido a la comprensión, pues muestra claramente cómo se pierde el control total de la imagen de una niña, evidenciando así el altísimo nivel de vulneración

³⁰ Secretaría General Iberoamericana, 25 de marzo de 2023.

³¹ Secretaría General Iberoamericana, 25 de marzo de 2023.

de sus derechos a la privacidad, a la reputación y a la autodeterminación informativa desde temprana edad.

Por otra parte, existen los riesgos de ciberacoso: la información compartida en línea puede propiciar que los niños sean objetos de situaciones de intimidación, acoso o burlas. Cuando se publican detalles privados de menores, que deberían haberse mantenido en estricta confidencialidad, o se comparten datos reveladores o vergonzosos, se les expone a sufrir de acoso por parte de sus pares y de muchas otras personas. Esta situación puede afectar terriblemente la vida de toda persona, mucho más la de un niño. En un estudio realizado en Estados Unidos con adultos que tienen discapacidades físicas y cognitivas, Haley señaló que los entrevistados expresaron serias preocupaciones debido a que sus padres han publicado en línea información sobre sus discapacidades desde su infancia. La mayoría argumentó que este contenido es extremadamente personal y, casi siempre, vergonzoso, lo que afectó negativamente su privacidad, identidad, estabilidad emocional y salud mental. Asimismo interfirió, y no para bien, en la forma en que sus pares se relacionaban e interactuaban con ellos³².

Relacionado con el aspecto anterior se encuentran los problemas emocionales y psicológicos: la sobreexposición online y el afianzamiento de la cultura de la validación a través de *likes* pueden desencadenar graves implicaciones en la estabilidad e integridad física, emocional y psicológica de las personas, en especial en los niños. También hay riesgos de cibervigilancia de datos: en razón de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, toda persona debe poder confiar en que los sistemas digitales que utilice, tanto en sus relaciones con el Estado como en su actividad económica, profesional, social o recreativa, serán seguros y resguardarán sus derechos a la privacidad y a la protección de datos, conforme al derecho interno. Sin embargo, en el informe del relator especial sobre el derecho a la privacidad de la Organización de las Naciones Unidas, se manifestó gran preocupación por la situación de la privacidad digital actual, pues con el pretexto del monitoreo requerido por la pandemia del covid 19, muchos gobiernos y actores privados entraron al campo de la cibervigilancia de datos personales, lo cual ha afectado negativamente el disfrute del derecho a la privacidad, a la personalidad y a otros derechos humanos conexos³³. Lo que antes se consideraba una sensación, ahora se ha evidenciado como una realidad que impulsa el modelo de la economía de datos. Algunos gobiernos³⁴, así como empresas estatales y

³² HALEY (2020), p. 1010.

³³ Organización de las Naciones Unidas, Asamblea General, 23 de julio de 2021.

³⁴ En el informe del relator especial sobre el derecho a la privacidad y la cibervigilancia

privadas enfocadas en la vigilancia de datos, recopilan millones de estos y crean perfiles individualizados. Estos son vendidos, transferidos, cedidos, transados, etcétera, a anunciantes, aseguradoras, agencias de empleo que, posteriormente, los utilizan en sus procesos de selección para otorgar o denegar servicios en sus respectivos campos. De esta manera, las clasificaciones realizadas por algoritmos de IA, alimentados con datos personales, determinarán con gran probabilidad el futuro de los niños. La vigilancia en línea puede impactar negativamente la posibilidad de que, en su vida futura, los menores califiquen para créditos universitarios, hipotecarios o de consumo; o sean seleccionados para determinados trabajos.

Y, finalmente, está la posibilidad de generar conflictos familiares: el *sharenting* y el *oversharenting* pueden provocar importantes conflictos en el núcleo familiar, especialmente si uno o varios miembros de la familia no están a favor de la exposición online de información personal o familiar. A medida que los niños crecen empiezan a considerar como una forma de intrusismo la publicación de su información personal por parte de sus padres. Haley hace mención a un estudio en el que se demuestra que un alto porcentaje de adolescentes estadounidenses rechaza o está en contra de que sus padres y otros familiares compartan información que ellos perciben como vergonzosa, siendo parte de esta categoría las fotografías de bebés desnudos o imágenes poco halagadoras; información que revela el mal comportamiento; información sobre sus amigos o sobre su vida amorosa³⁵.

Haciendo un inciso en este punto, podemos traer a colación el caso del bebé Nevermind, quien ha manifestado afectación de su salud mental y estabilidad emocional como adolescente y como adulto, dado el bochorno que representa para él la fotografía en la que está totalmente desnudo. Alegando, además, que la misma existe gracias a la anuencia de sus padres, pero fue publicada sin su consentimiento, y que ha enriquecido a la banda y a todos los involucrados de su entorno. Este caso plantea muchos dilemas, entre ellos, la privacidad como componente esencial para la construcción de un vínculo socioafectivo sano y sólido entre padres e hijos.

masiva, se muestra una preocupación especial con los gobiernos de: China, Rusia, Irán, Singapur, India y Estados Unidos.

³⁵ HALEY (2020), p. 1011.

III. CONFLICTOS ENTRE EL DERECHO DE PATERNIDAD/MATERNIDAD, LA LIBERTAD DE EXPRESIÓN DE LOS PADRES Y EL DERECHO A LA PRIVACIDAD DE LOS HIJOS

El derecho de paternidad/maternidad refiere al conjunto de derechos y responsabilidad que los padres tienen respecto de sus hijos. En esencia, estos tienen por objeto garantizar el bienestar, protección y desarrollo íntegro de los hijos. Algunos aspectos fundamentales de este derecho son la garantía de reconocimiento de una relación jurídica entre padres e hijos; el derecho y obligación de cuidado, educación y establecimiento de un ambiente amoroso y seguro donde el niño pueda desenvolverse lo más íntegramente posible; el derecho de convivir con los hijos, siempre que sea en beneficio de estos; el deber de protección de los niños de cualquier forma de maltrato, abuso o negligencia; el derecho y responsabilidad de cubrir las necesidades básicas de subsistencia de los hijos; la facultad de tomar decisiones sobre la crianza —educación, religión, salud, rutina, etcétera—; y el derecho de compartir experiencias, méritos y momentos familiares especiales como una forma de extensión de la libertad de expresión.

No obstante, este derecho no es absoluto y tiene limitaciones, especialmente, cuando se contraponen a los derechos de los hijos. En la era digital este conflicto es más evidente, pues se pone de manifiesto la tensión entre el deseo de los padres de ejercer su paternidad/maternidad y la obligación de protección de los derechos de privacidad de los hijos. En el contexto actual los padres, en ejercicio de su libertad de expresión, comparten experiencias, logros, momentos, en las plataformas digitales. Pero al hacerlo, voluntaria o involuntariamente podrían vulnerar los derechos a la privacidad y protección de datos de sus hijos, quienes no han otorgado su consentimiento para esa exposición. Ese escenario se complica cuando la información publicada genera una situación de vulnerabilidad para los niños. Por tanto, esta situación plantea un dilema ético y legal en la que es imperativo trazar el límite entre el derecho de los padres a ejercer libremente su paternidad/maternidad y su derecho a la libertad de expresión; y el derecho inherente del niño a la privacidad y a su autodeterminación informativa en el presente y en el futuro.

En tal sentido, y siguiendo las recomendaciones establecidas en la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, la corresponsabilidad digital desempeña un rol fundamental³⁶. En la medida en que todos los actores involucrados en el ecosistema digital —personas, gobiernos, empresas y organizaciones civiles— asuman que este exige de

³⁶ Secretaría General Iberoamericana, 25 de marzo de 2023.

una responsabilidad compartida, se podrán generar más espacios seguros en internet, con ética y respeto por los derechos humanos en la mayor medida posible. Esto implica que cada parte debe contribuir activamente a la protección de datos, la privacidad, la ciberseguridad y el uso consciente de la tecnología, en especial cuando hay menores involucrados.

Sin lugar a dudas, la corresponsabilidad digital es trascendental en este mundo interconectado, donde las acciones de uno pueden afectar a muchos, tanto en el presente como en el futuro, incluso de formas inimaginables. Es especialmente importante insistir en que los menores, por ser un grupo particularmente vulnerable, deben estar protegidos por un sistema especial que garantice sus derechos e intereses superiores.

1. El interés superior del niño como fundamento de defensa de su privacidad digital

Tradicionalmente, se ha considerado que el derecho a la privacidad de los niños debe ser gestionado a criterio de los padres. Sin embargo, las necesidades de privacidad de los menores pueden diferir de las de sus padres e, incluso, pueden llegar a estar en conflicto, por ejemplo, cuando la divulgación de información sobre los hijos pone en conflicto la libertad de expresión de los padres con el derecho a la privacidad de los primeros. En el derecho internacional, la definición de niño está plenamente estipulada. En su artículo 1, la Convención sobre los Derechos de los Niños (1989) establece que se «entiende por niño todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad»³⁷. Asimismo, la Convención plantea que las garantías circunscritas a su ámbito de protección resguardan a los niños desde su nacimiento hasta la mayoría. Esta precisión ofrece un marco unificado para entender y abordar los derechos de los niños a nivel global.

La Convención establece en su preámbulo las razones por las cuales debe prevalecer el interés superior del niño, fundamentándose que este requiere de cuidados especiales. En concreto instituye que: «*El niño, por su falta de madurez física y mental, necesita protección y cuidado especiales, incluso la debida protección legal, tanto antes como después del nacimiento*»³⁸. También, en su artículo 14.1 indica que «*los Estados Partes respetarán el derecho del niño a la libertad de pensamiento, de conciencia y de religión*»; y en su artículo 16.1 instituye que «*ningún niño será objeto de injerencias*

³⁷ Organización de las Naciones Unidas, 20 de septiembre de 1989, Convención sobre los Derechos de los Niños.

³⁸ Organización de las Naciones Unidas, 20 de septiembre de 1989, Convención sobre los Derechos de los Niños, párrafo 9.

arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación»³⁹.

De lo anterior se desprende que los niños, desde su nacimiento hasta su mayoría, son titulares de pleno derecho al honor, a la reputación y a la privacidad personal y familiar. Además, la Convención confiere el mandato a los gobiernos —Estados parte— la garantía de su protección. Además, en el derecho hemisférico americano —Convención Americana sobre Derechos Humanos (Pacto de San José)— se establece en su artículo II, en sentido general, sobre la protección de la honra y de la dignidad que: «1. *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.* 2. *Nadie puede ser objeto de injerencias arbitrarias y 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»⁴⁰. En adición, podemos observar lo estipulado en su artículo 19, que especifica sobre los derechos del niño que «*todo niño tiene derecho a las medidas de protección que su condición de menor requieren por parte de su familia, de la sociedad y del Estado»⁴¹.**

En todo caso, la Convención Americana es clara al estipular que la imperatividad de adoptar medidas o cuidados especiales respecto de los niños obedece a la situación específica en la que se encuentran, considerando su debilidad, su inmadurez y su inexperiencia. También, es importante referir lo contemplado en el derecho comunitario europeo. Si bien en este no se ha desarrollado amplia y expresamente un marco legal protector especializado en los menores, si debe considerarse que, de momento, es el sistema internacional que mayor nivel de actualización tiene en el tema. Encontramos en este varias normativas destinadas a garantizar el derecho a la privacidad de los niños en el ciberespacio. Entre ellas destacan el RGPD⁴², que de forma general instituye la protección de datos personales de todos los ciudadanos de la Unión, pero también especifica disposiciones de protección digital de los menores. Por ejemplo, en el artículo 8.1 —referente a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información— los

³⁹ Organización de las Naciones Unidas, 20 de septiembre de 1989, Convención sobre los Derechos de los Niños.

⁴⁰ Organización de los Estados Americanos, 22 de noviembre de 1969, Convención Americana sobre Derechos Humanos.

⁴¹ Organización de los Estados Americanos, 22 de noviembre de 1969, Convención Americana sobre Derechos Humanos.

⁴² Unión Europea, 27 de abril de 2016, reglamento 679.

menores de 16 años requieren del consentimiento del titular de la patria potestad o tutela para que se procesen sus datos en ciertos contextos.

Destaca también en este ámbito la Directiva ePrivacy⁴³, sobre la privacidad y las comunicaciones electrónicas, en la que se garantizan los derechos relativos a la privacidad, a la confidencialidad y a las reglas de la comercialización directa en la que estén implicados datos personales. Si bien su régimen protector se expone en sentido general y no específico para los menores, de forma implícita se asume que estos últimos están incluidos en su ámbito de protección. Otro instrumento destacable es la Directiva sobre los derechos de los consumidores⁴⁴, que aun cuando no se centra en el tema de la privacidad, tiene algunas disposiciones que protegen a los consumidores en internet, incluidos los menores, acerca de la información que debe proporcionarse al realizar una compra o en referencia al derecho de desistimiento. De igual modo, resalta la Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil⁴⁵, en la que se busca protegerlos de los peligros propios de internet, lo que de forma directa incide en la protección de su privacidad y seguridad en el ciberespacio.

Asimismo, es relevante el Bik+ o Brazo digital de la estrategia global de la Unión Europea sobre los derechos del niño⁴⁶. Esta estrategia se enfoca en mejorar las experiencias en línea de los menores, abordando temas como el contenido pernicioso o perjudicial, la publicidad y la promoción de la alfabetización digital. Para ello propone tres campos puntuales de actuación: i) la generación de experiencias digitales que protejan a los niños de los riesgos de internet; ii) el empoderamiento digital de los niños; iii) su participación fundada en el respeto de su dignidad.

Aplicando estas precisiones al *sharenting* y al *oversharenting*, puede indicarse que la Convención de los Derechos de los Niños, la Convención Americana y los demás instrumentos jurídicos internacionales aplicables suponen como *conditio sine qua non*, de forma implícita, que para compartir información referente a un niño debe contarse con el consentimiento de este y el de sus padres. Además de que, en principio, de forma previa a que los padres o adultos responsables del menor publiquen su información en internet, deberían preguntar y solicitar su autorización. En casos

⁴³ Unión Europea, 12 de julio de 2002, Directiva 58.

⁴⁴ Unión Europea, 25 de octubre de 2011, Directiva sobre los derechos de los consumidores.

⁴⁵ Unión Europea, 13 de diciembre de 2011, Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

⁴⁶ Comisión Europea, 24 de febrero de 2021, Estrategia sobre los derechos del niño.

de menores sin la madurez y capacidad de discernimiento suficiente, debería contarse con la autorización de ambos padres, o en casos más extremos, dadas las circunstancias de cuidado o tenencia de la patria potestad, debería contarse con una autorización judicial. Esta argumentación, que puede parecer excesiva o extrema, no es tal si se toma en cuenta el interés superior del niño, una premisa fundamental en todos los tratados y convenciones internacionales relacionados con sus derechos.

Actualmente, los padres, familiares, amigos o cercanos difunden en plataformas digitales o en otros medios relacionados imágenes, videos, opiniones y, en general, información personal de menores, revelándose con ello datos o episodios vergonzosos, desagradables o propios de la intimidad, personal o familiar del menor. Además, considerando que actualmente el modelo de economía de los datos se caracteriza por su masificación, por la permanencia indefinida de la información en la memoria digital y por dilemas éticos planteados por el tratamiento de datos personales; surgen preocupaciones válidas sobre los peligros y repercusiones presentes y futuras en la privacidad y la dignidad de los menores en el espacio digital. Por tanto, es en extremo necesario adoptar medidas cautelares que garanticen y protejan sus derechos en esta realidad de hiperconexión global.

IV. EL DERECHO AL OLVIDO COMO MECANISMO DE ALIVIO DE TENSIONES ENTRE DERECHOS

Como se ha dicho, el *sharenting* consiste en una práctica parental mediante la cual se comparte, a través de plataformas digitales, información personal de un niño sin su consentimiento y, en algunos casos, se hace con fines económicos. Esta práctica puede conducir a un conflicto jurídico, como lo evidencian los casos *Nevermind baby* y *Jinmiran baby*. Sin embargo, acá no solo están involucrados los intereses de los niños, pues cuando los padres o adultos responsables del menor comparten videos, fotos, historias en redes sociales, no están mostrando solamente una información referente a sus hijos o tutelados, también están relatando sus vivencias como padres. En tal sentido, cabe reflexionar sobre los límites en los que empieza y termina la identidad de los padres, y lo mismo, para los hijos.

La cuestión a resolver, entonces, es cómo conciliar el legítimo anhelo de los padres de compartir y preservar momentos de la infancia de sus hijos y de su experiencia como padres con el respeto a la protección de la privacidad de los datos personales de los niños. El derecho al olvido puede ser uno de los instrumentos jurídicos a considerar dentro de las estrategias

posibles. Este ha emergido como un derecho fundamental, puntualmente en el derecho comunitario europeo y, aunque en menor medida, en otros sistemas jurídicos. Desde su reconocimiento ha afrontado notables desafíos, sobre todo en lo relacionado con la recolección, almacenamiento, tratamiento y masificación de datos personales, especialmente los de naturaleza sensible⁴⁷.

Este derecho otorga a las personas, bajo determinados parámetros y siempre que se cumplan algunas condiciones, la facultad de solicitar suprimir información personal de los resultados de los motores de búsqueda en internet. Para ello debe cumplirse: i) que exista vulneración a los derechos de privacidad y protección de datos; ii) que esa vulneración afecte al ejercitante, principalmente, en lo que respecta a su reputación, imagen u honor; y iii) que no se afecten derechos de terceros —individuales o colectivos—, particularmente, los que refieran a la libertad de información y libre expresión, aunque en dicho caso, es esencial recurrir a la ponderación jurídica correspondiente.

Para consolidar la implementación del derecho al olvido se requiere de un equilibrio entre, por un lado, los derechos y libertades referentes al acceso a la información y, por otro, la garantía de los derechos a la privacidad y protección de datos. Así, los sistemas legales que lo garantizan —o al menos, así sucede en el derecho comunitario europeo— buscan resguardar un equilibrio entre la garantía de los derechos a la privacidad, protección de datos personales y el acceso a la información. No obstante, la naturaleza y alcance de protección del derecho al olvido generan controversias y debates relevantes que son fundamentales para abordar dilemas jurídicos y éticos sobre la protección de los derechos humanos y, especialmente, acerca de la privacidad, los datos personales y la preservación de la memoria histórica.

1. Comprendiendo el derecho al olvido

El derecho al olvido digital es nuevo y es *in fieri*, es decir, es un derecho en proceso de formación, definición y consolidación en el ámbito jurídico. Se entiende que está en constante evolución, dada su naturaleza dinámica y cambiante y su contenido, objeto de protección y aplicabilidad que varía entre sistemas jurídicos y contextos sociales. Mientras que en algunos Estados se ha reconocido el derecho al olvido como fundamental, a través de normas específicas, tal como sucede en el derecho comunitario europeo, en otros países su reconocimiento es limitado, exiguo o inexistente. Esta

⁴⁷ MOLINA LUNA Y BENFELD (2022), p. 658.

variabilidad evidencia el continuo desarrollo *iustificable* del derecho al olvido y la sujeción respecto de la evolución legal y social.

Este derecho surge como respuesta a los desafíos planteados por la digitalización, en particular, el almacenamiento, disponibilidad, tratamiento y circulación de información personal en internet. Históricamente, las personas han proporcionado información en diversos contextos: entidades bancarias; sistemas educativos; trámites legales; atención sanitaria; actividades comerciales; etcétera. Esto se sustenta en la premisa de una suerte de *pacto social* implícito, en que los individuos han cedido partes de privacidad para que, hasta cierto punto, la sociedad opere dentro de un sistema de reglas jurídicas.

En este sentido, es importante reflexionar sobre la expectativa razonable de privacidad en el contexto digital actual. Tradicionalmente, se ha asumido, al menos en la cultura occidental, que los niveles básicos de privacidad y confidencialidad deben respetarse dentro de los límites legalmente establecidos. No obstante, en esta era de masificación de la información y de vigilancia constante, esta idea implicaría que, aunque los datos personales se recopilen y almacenen rutinariamente, las personas siempre tienen el derecho de esperar que estos no sean empleados indebidamente, divulgados sin su consentimiento, ni tratados con fines desconocidos o distintos a los previstos inicialmente.

En principio, esta expectativa razonable de privacidad debería incluir la protección contra la recopilación excesiva de datos, el derecho de conocer cómo se emplearán sus datos y, sobre todo, tener la posibilidad de controlar y corregir la información personal disponible en internet. Aun cuando son evidentes los desafíos de la era digital, la expectativa razonable de privacidad es imprescindible para mantener la confianza en las interacciones digitales y proteger la dignidad y los derechos de las personas. Sin embargo, la digitalización ha sobrepasado esta expectativa razonable de privacidad. Información personal que anteriormente estaba resguardada en archivos físicos y bajo códigos de confidencialidad, ahora se encuentra en una memoria digital ilimitada y, de momento, perpetua.

Agravando la situación, mucha de esa información se encuentra, en la mayoría de los casos, en posesión de entes privados cuyo objetivo principal es lucrar o de gobiernos autocráticos, tiránicos o dictatoriales. Además, a estos datos se suman innumerables registros privados que, cada segundo, están siendo recopilados por las *big tech* sin el consentimiento del titular. Complicando aún más el panorama, estos datos son vendidos, cedidos o transferidos sin consentimiento, o sin una protección jurídica robusta que resguarde el tratamiento de datos personales y la privacidad.

Aunque existen avances legislativos y judiciales en la protección de datos personales y de la privacidad, no existe uniformidad, reciprocidad, ni colaboración global. Esa falta de cohesión refleja el imperativo de resolver estas lagunas en la protección de los derechos personales en el espacio digital. Todo ello ha generado una creciente demanda social que exige la protección de los derechos personales en internet. El derecho al olvido es un ejemplo de ello. Este surge, propiamente tal, en 2016 tras la convergencia de varias causas comparables⁴⁸, entre las que destaca el caso *Mario Costeja-AEPD vs Google Inc.*⁴⁹.

2. *El derecho al olvido como instrumento de alivio de tensiones entre padres e hijos*

Internet, y en especial las redes sociales, conllevan la exigencia de formas específicas de protección de los derechos humanos y fundamentales a las que la doctrina y parte importante de los sistemas jurídicos en el mundo han denominado derechos digitales, dentro de los cuales se encuentra el derecho al olvido. Como se ha visto, este cobra especial relevancia en la medida en que la información personal aumenta vertiginosamente en internet y permanece indefinida e ilimitadamente en una abstracción virtual: la memoria digital. En tal sentido, este derecho se convierte en una cuestión trascendental pues cualquier información personal podría encontrarse por medio de cualquier forma de búsqueda en internet. Actualmente, con la ayuda tecnológica, olvidar se ha vuelto la excepción, y recordar la configuración por defecto⁵⁰. Con enormes cantidades de información personal disponible y al alcance de un clic en internet, se propicia un contexto de vulnerabilidad en el que hay pocas posibilidades de redención, de perdón o de derecho a una segunda oportunidad.

En ese orden, adquiere especial importancia el derecho al olvido para los menores como «una prerrogativa reconocida por el [RGPD] de la Unión Europea en su artículo 17»⁵¹. Considerando lo anterior, en adición de lo establecido en los considerandos 38 y 65 del RGPD, las personas pueden solicitar a los motores de búsqueda de internet y a la fuente de la publicación original —bien sea cuentas personales o corporativas de plataformas digitales, o a otros sitios web o blogs— la supresión de

⁴⁸ MOLINA LUNA y BENFELD (2022), p. 659.

⁴⁹ Tribunal de Justicia de la Unión Europea (2014), asunto *Google Spain-Google Inc. y AEPD vs Mario Costeja González*.

⁵⁰ MAYER-SCHÖNBERGER (2009), p. 15.

⁵¹ KOPECKY *et al.* (2021), p. 4.

información personal referida a su niñez, compartida por iniciativa propia o por terceras personas.

Incluso, autoras como Haley van un paso más allá y afirman la necesidad de reconocer una modalidad especial de derecho al olvido: el derecho al olvido para los menores, manifestando que los niños y adolescentes deben tener siempre la posibilidad de requerir la eliminación de cualquier información personal referente a ellos mismos⁵². En esa misma línea, Bessant *et al.* establecen que es necesario introducir una mejora en el reconocimiento genérico del derecho al olvido, para poder garantizar que las solicitudes hechas por menores para eliminar información personal —que ha sido compartida por sus padres o por terceros— sea aceptada por Facebook, Instagram, WhatsApp o YouTube⁵³.

Pero, ¿puede realmente el derecho al olvido digital mitigar las tensiones entre padres e hijos a propósito del *sharenting* y *oversharenting*? Sobre el primero, Haley defiende que el derecho al olvido puede aliviar las tensiones entre los derechos de los padres y los intereses de los niños y, además, también permite equilibrar los intereses en juego de unos y otros en las redes sociales⁵⁴. Dentro de ese mismo paradigma, Steinberg, coincidiendo con Haley, establece que el derecho al olvido de los niños podría ofrecer la solución que muchas familias necesitan para resolver problemas generados por los efectos indeseados del *sharenting* y el *oversharenting*⁵⁵.

Acorde con lo expuesto hasta ahora y coincidiendo con Haley y Steinberg, el derecho al olvido si puede entenderse como un recurso legal para mitigar tensiones, entre padres e hijos, generadas por efectos no previstos o no deseados del *sharenting* y del *oversharenting*. Este derecho puede facilitar la autonomía de la identidad digital del menor, permitiéndoles solicitar la desvinculación de información que vulnere su privacidad, identidad o reputación. Además, esto coadyuba en la resolución de conflictos que pueden aparecer cuando los jóvenes crecen y se concientizan sobre su identidad personal, asumiendo que la información expuesta por sus padres no representa su propio sentido del *yo*. En segundo lugar, el derecho al olvido puede asumirse como un instrumento del derecho de protección de datos personales ante el acoso y la vergüenza. Esto puede significar, para muchos menores, el medio a través del cual logren superar episodios de degradación de su dignidad. En tercer lugar, el derecho al olvido puede permitir, en cierta medida, la limpieza de la huella y reputación digital.

⁵² HALEY (2020), p. 1007.

⁵³ BESSANT *et al.* (2020), p. 10.

⁵⁴ HALEY (2020), p. 1015.

⁵⁵ STEINBERG (2017) p. 842.

De esta manera, podrían disminuir las situaciones de discriminación y vulnerabilidad a las que podrían estar expuestos con consecuencias como la denegación de un puesto de trabajo, de un seguro médico, del otorgamiento de una beca de estudio, etcétera.

No obstante, también deben observarse los desafíos. Aun cuando el derecho al olvido significa un medio de mitigación de las tensiones existentes entre padres e hijos a propósito del *sharenting* y el *oversharenting*; de igual modo debe considerarse que no es una solución completa o plenamente efectiva. La realidad que debe enfrentarse al momento de ejercerlo es que es muy difícil su implementación debido a las dificultades asociadas a su uso, entre las que encontramos⁵⁶ la imposibilidad para determinar la variabilidad y relatividad del tiempo que debe transcurrir para considerar que una información ya no es pertinente o vigente; como asimismo la complejidad para determinar hasta qué punto se puede permitir el anonimato o la disminución de la exposición de datos de una figura pública (producto de un cargo político, participación en actividades artísticas o periodísticas, etcétera). Esto, pues pudo generarse mucha información asociada a sus datos personales y a su vida privada que puede considerarse parte importante del acervo histórico, cultural, económico, político, social, artístico, etcétera.

Otra dificultad es que podría ser una acción poco expedita, infructuosa y de complicada implementación al requerir la intervención de la autoridad en materia de protección de datos, generalmente, de una agencia de protección de datos. En este sentido, puede ser un derecho bastante oneroso si se contrata un servicio privado para efectuar el procedimiento y resolverlo en menos tiempo que el responsable del tratamiento de los datos, o en caso de negativa de este, la agencia de protección de datos.

Además, en la práctica, la implementación del derecho al olvido ha significado conferir a corporaciones privadas el poder de decidir qué debe —y qué no— aparecer en internet. Esto no es compatible con los valores democráticos de un genuino Estado de derecho, y no resulta esperanzador, dado que en los últimos años estas corporaciones han sido cuestionadas por prácticas bastante distantes de la ética. Además, en ningún caso este derecho supone la eliminación, rectificación o modificación de las fuentes originales donde se publicó la información. En lugar de ello, la norma permite que dicho contenido permanezca oculto en los resultados de búsqueda, haciéndolo difícil de encontrar. Es decir, aunque la información permanece en su fuente original, ya no será posible vincularla con los datos personales del titular.

⁵⁶ MOLINA LUNA Y BENFELD (2023) p. 30.

Ejercer este derecho es complicado porque, además, el funcionamiento de internet se basa en la vinculación de enlaces entre sitios web. Si bien Google es el más empleado, no es el único. Existen otros buscadores como: Yahoo, Bing, Baidu, Ask, Ecosia, DuckDuckGo y Yandex. Por tanto, para que el derecho al olvido sea efectivo, el interesado debe extender su pretensión a varios motores de búsqueda. En este sentido, cabe recordar que el derecho al olvido es útil para esconder en internet información que vulnera derechos humanos, pero no repara totalmente —desde los derechos humanos— las lesiones jurídicas. Incluso, en muchos casos se genera el efecto Streisand: después de que la solicitud ha sido aceptada, la información puede encontrarse por otros medios, lo que sigue exponiendo al solicitante a vulneraciones de derechos, como se evidenció con el caso *Mario Costeja con Google*.

Finalmente, cabe tener presente que el derecho al olvido no es ilimitado ni absoluto. La decisión de desvinculación de enlaces de buscadores y sitios web que alojan información sobre una persona no debe dejarse exclusivamente a la voluntad del afectado pues, aunque puede reparar derechos transgredidos, también podría privilegiar derechos del afectado sobre otros, como los derechos a la información, la libertad de expresión y la libertad de prensa. En definitiva, según el artículo 17 del RGPD, el derecho al olvido no se trata en *strictu sensu* de un derecho a la autodeterminación informativa o a la personalización del perfil digital del afectado⁵⁷.

En resumen, el derecho al olvido ofrece una solución para proteger la privacidad y los datos personales de los menores en el espacio digital luego de una transgresión. Gracias a este, se puede recuperar, en cierta medida, el control sobre la presencia digital y la privacidad. Sin embargo, no aborda completamente el problema central del *sharenting* y el *oversharenting*. Además, su implementación puede generar nuevos desafíos.

V. CONCLUSIONES

El avance tecnológico digital y el modelo de economía de datos han transformado nuestras comunicaciones e interacciones, normalizando la sobreexposición en el espacio digital. Esto ha propiciado fenómenos como el *sharenting* —personal o monetizado— y el *oversharenting*, que pueden

⁵⁷ A pesar de que a su alrededor ha surgido un gran negocio que se evidencia con empresas como: Borrame.es; Navascusi.com; Tuabogadodefensor.com; Eliminalia.com; Openley.es; Reputacion.com; Audea.com; ePrivacidad; Abanlex.com; Reputación en Internet o Abine; TeBorramos; Honoralia; RepScan; Eliminalo.cl.; Internet Reputation; DeteleMe; Deseat.Me.

tener implicaciones serias, especialmente con los menores. La publicación en exceso de información personal de niños, ya sea intencionalmente, por ingenuidad o desconocimiento, puede comprometer su seguridad y dignidad. Proteger a los niños en el ciberespacio no es solo cumplir con normativas legales, sino también expresar los valores morales y éticos de nuestra sociedad. Esta realidad digital plantea desafíos significativos, enfatizando la necesidad urgente de adoptar medidas de protección que garanticen el bienestar de los niños en la realidad virtual. En respuesta a estas circunstancias, surge el derecho al olvido, reconocido como fundamental en el artículo 17 del RGPD tras el caso de *Mario Costeja con Google*. Este derecho establece la necesidad de proteger la privacidad y los datos personales en internet, permitiendo que las personas soliciten la desindexación de información personal irrelevante, incorrecta, obsoleta, improcedente o que no corresponda al propósito original de recolección.

Este estudio sugiere algunas reflexiones sobre la intersección entre el *sharenting*, el *oversharenting* y la protección que el derecho al olvido representa para la privacidad y los datos personales de los menores. Una de ellas es que existe un consenso legal internacional —Convención de los Derechos de los Niños, Convención Americana, e instrumentos jurídicos de la Unión Europea— y un consenso doctrinario que reconocen a los niños como titulares de los derechos al honor, privacidad y protección de datos personales; asimismo, podemos concluir que dada su vulnerabilidad, los menores tienen un sistema de protección especial enmarcado en la responsabilidad digital, basado en el interés superior del niño, principio que prevalece sobre derechos de terceros en situaciones de conflicto. También, debemos considerar que los niños expuestos al *sharenting* y *oversharenting* enfrentan riesgos que impactan su desarrollo personal, su integridad física y mental, así como su privacidad e imagen personal; y que, aunque los padres son conscientes de los riesgos de la divulgación de información personal de sus hijos, la frecuencia de esta práctica va *in crescendo*, lo que demuestra la necesidad de apoyo externo para que los menores puedan solicitar la supresión de contenido publicado sin su consentimiento.

Asimismo, podemos indicar que la percepción de la imagen propia o reputación, y lo que se considera público y privado, es versátil y tiende a la transformación, lo que subraya la importancia del cuidado que se debe tener al compartir contenido en el ciberespacio, especialmente cuando se trata de menores, ya que lo publicado en internet puede perdurar indefinidamente. En este sentido, se presume, en principio, que los menores puede solicitar el derecho al olvido a través de sus padres o representantes legales. No obstante, ¿qué ocurre cuando son los propios padres o repre-

sentantes legales quienes (sobre) exponen la imagen del menor en el ciberespacio? ¿Existe claridad sobre la importancia del consentimiento y del respeto a los derechos personales de los niños en esas circunstancias? Estas interrogantes requieren respuestas urgentes. De la mano con lo anterior, podemos afirmar que los efectos graves del *sharenting* y *oversharenting* destacan la necesidad de redefinir el rol de los padres y adultos responsables en la preservación de la privacidad de los menores, tanto en la realidad digital como en la analógica.

Otro tema que se debe considerar en esta materia es que la información que se comparte constantemente en internet constituye un recurso invaluable para las *big tech*, anunciantes, empresas de marketing, plataformas digitales y políticos, quienes utilizan los datos personales para crear perfiles sociodemográficos detallados —huellas digitales— lo que tiene implicaciones serias, especialmente para la generación actual: *centennials* y *pandennials*, cuyo rastro digital se construye desde temprana edad e incluso antes de su nacimiento. En concreto, empresas como Google, Facebook, Instagram, TikTok, Twitter (X), YouTube, Apple, Amazon, Microsoft y muchas más, poseen millones de perfiles de niños, adolescentes y jóvenes, recopilados desde su nacimiento o antes. Esta información no solo les confiere una omnipresencia tecnológica, en términos de George Orwell, sino también la capacidad de influir en las emociones y vulnerabilidades según sus estándares éticos y metas económicas.

Otra reflexión importante es que el derecho al olvido es un instrumento de protección que permite mitigar tensiones entre los derechos de los menores: privacidad, datos personales y reputación; y los derechos de los padres: paternidad/maternidad, libertad de expresión, etcétera. Permite al titular de los datos retomar cierto control de su información personal y resguardar su privacidad, aunque no soluciona el problema central: el *sharenting* y el *oversharenting*. De hecho, el derecho al olvido tiene limitantes significativas en su operatividad y efectividad. No permite borrar la información de la fuente original donde fue publicada sino que solo desvincula, en los motores de búsqueda, los datos personales de la información y continúa la posibilidad de su recuperación por otras formas de búsqueda.

Es imprescindible, entonces, que todos reflexionemos antes de compartir información personal en internet, especialmente cuando se trata de menores, considerando el impacto en la libertad de elección y el consentimiento de los involucrados. Esto es relevante, particularmente, para los padres, tutores legales y cuidadores, cuyas acciones repercuten y afectan ampliamente el desarrollo integral de los niños. Junto a esto, es trascendental promover la educación y concienciación sobre prácticas seguras de uso

de internet, dando prioridad a la protección de la privacidad y la seguridad de los niños. En este sentido, los casos de Nevermind y Jinmiram baby ejemplifican los dilemas éticos, morales y jurídicos generados desde el rol de los padres como responsables en un mundo interconectado. Es necesaria la concientización sobre los riesgos del *sharenting* y *oversharenting*, que incluyen la transgresión de la privacidad; la pérdida de control de la información; la vulnerabilidad de la identidad digital; la afectación a la reputación digital; la cibervigilancia; problemas emocionales, psicológicos y familiares; la exposición a delincuentes y riesgos de ciberacoso, entre otros.

Finalmente, creemos que debe crearse una cultura jurídica de corresponsabilidad digital que valore el consentimiento del niño como *conditio sine qua non* para realizar cualquier publicación que implique su información personal. Actualmente, existen pocas herramientas efectivas para proteger los derechos en internet y el derecho al olvido, aunque útil en algunos casos, no repara completamente el daño causado. Es crucial la concientización sobre las repercusiones presentes y futuras de la información compartida en línea. De momento, limitar la exposición de los menores en plataformas digitales, solicitar su opinión y consentimiento para compartir información, y tener un control estricto de la privacidad en redes sociales pueden ser medidas preventivas.

En términos de Véliz, «vivimos en casas de cristal y mientras más sepan de nosotros más expuestos y vulnerables somos»⁵⁸. Esto empeora en el caso de los menores. Como han señalado Francis Bacon, Thomas Hobbes, Michel Foucault, y tantos otros, siempre ha existido una relación íntima entre conocimiento y poder, lo que plantea un problema colectivo y trascendental, más allá de las corporaciones tecnológicas o los gobiernos, pues la abundancia de información digital nos expone de manera sin precedentes, especialmente a los niños. En consecuencia, la evolución de la tecnología digital, aunque es uno de los grandes logros y avances de la humanidad, también representa una potencial amenaza para los derechos personales, especialmente para los niños. Es crucial salvaguardar derechos como la privacidad, la protección de datos, la identidad, la reputación y la autodeterminación informativa a través de marcos normativos que evidencien el establecimiento de principios genuinos de corresponsabilidad digital. Es necesario, no solo que se regulen las actuaciones estatales y las acciones de las empresas tecnológicas, sino también que se establezcan deberes y responsabilidades hacia las familias en general, en vista de que los niños son vulnerables a diversos delitos en internet.

⁵⁸ VÉLIZ (2020), p. 103.

BIBLIOGRAFÍA CITADA

- Ayten, Keskin, Nazan, Kaytez, Mustafa, Damar, Fatma, Elibol y Neriman Aral (2023): «Sharenting syndrome: An appropriate use of social media?», en: *Healthcare*, Vol. 11, N° 10: pp. 1-17: [DOI <https://doi.org/10.3390/healthcare11101359>].
- 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», en: *Revista Internacional de Información y Comunicación*, Vol. 27, N° 1: pp. 27-35.
- Benfeld, Johann (2023): *Una cuestión de fidelidad: Sobre el ethos de la profesión legal* (Valparaíso, Ediciones Universitarias de Valparaíso).
- Bessant, Claire, Nottingham, Emma y Oswald, Marion (2020): «Sharenting in a socially distanced world», en: *London School of Economics*, N° 12: p. 10. Disponible en: <https://tipg.link/gCsV> [Fecha de consulta: 19.1.2024].
- Boyd, Danah (2011): «Social network sites as networked publics: Affordances, dynamics, and implications», en: Papacharissi, Zizi (editora), *A networked self: Identity, community, and culture on social network sites* (Nueva York-Londres, Routledge), pp. 39-59.
- Davara Fernández, Laura (2017): *Menores en internet y redes sociales: Derecho aplicable y deberes de los padres y centros educativos* (Madrid, Boletín Oficial del Estado).
- (2021): *El libro definitivo sobre redes sociales: Claves para padres y educadores* (Ciudad de México, Cuadernos de Pedagogía).
- Haley, Keltie (2020): «Sharenting and the (potential) right to be forgotten», en: *Indiana Law Journal*, Vol. 95, N° 3: pp. 1006-1020.
- Hall, Holly (2018): «Oversharenting: Is it really your story to tell?», en: *J. Marshall J. Info. Tech. & Privacy*, Vol. 33, N° 121: pp. 120-142. Disponible en: <https://tipg.link/gCu2>.
- Holzer, Natalia (2017): «Oversharing: Padres que comparten en exceso en redes sociales. Dimensiones éticas y antropológicas de la cuestión», en: *Revista Palabras*, N° 1: pp. 92-106. Disponible en: <https://tipg.link/gCuG>.
- Klucarova, Sona y Hasford, Jonathan (2021): «The oversharenting paradox: When frequent parental sharing negatively affects observers' desire to affiliate with parents», en *Current Psychology*, Vol. 42, N° 1: pp. 1-11: [DOI <https://doi.org/10.1007/s12144-021-01986-z>].
- Kopecky, Kamil, Szotkowski, Rene, Aznar, Inmaculada y Romero, José (2021): «Sharenting y derechos digitales de los niños y adolescentes», en: *Profesional de la Información*, Vol. 30, N° 4: pp. 1-10.

- Mayer-Schönberger, Viktor (2009): *Delete: The virtue of forgetting in the digital age* (Princeton, Princeton University Press).
- Molina Luna, Maryori y Benfeld, Johann (2022): «Derecho de supresión de datos (“Derecho al olvido”): Antecedentes jurisprudenciales que explican los fundamentos del reconocimiento de este nuevo derecho en el sistema jurídico de la Unión Europea», en: *Revista Rechtsstaat, Estado de Derecho*, N° 1/especial: pp. 656-689.
- (2023): «Surgimiento y evolución del derecho de supresión de datos personales en motores de búsqueda de internet (derecho al olvido): Una mirada desde el derecho español y su proyección hacia el derecho comunitario europeo», en: *Revista Chilena de Derecho y Tecnología*, Vol. 12: pp. 1-36: [DOI <https://doi.org/10.5354/0719-2584.2023.67594>].
- Muhammad, Saud, Musta'in, Mashud y Rachmah, Ida (2020): «Usage of social media during the pandemic: Seeking support and awareness about covid-19 through social media platforms», en: *Journal of Public Affairs*, Vol. 20, N° 4: DOI [<https://doi.org/10.1002/pa.2417>].
- Ordóñez, Luis y Calva, Stefany (2020): «Amenazas a la privacidad de los menores de edad a partir del sharenting», en: *Revista Chilena de Derecho y Tecnología*, Vol.9, N° 2: pp. 105-130: DOI [<https://doi.org/10.5354/0719-2584.2020.55333>].
- Plunket, Leah (2019): *Sharenthood: Why we should think before we talk about our kids online* (Massachusetts/Londres, The MIT Press).
- South Australia Commissioner for Children and Young People (2020): «Fact sheet manage your sharenting», en: *Commissionercyp online*, p. 3. Disponible en: <https://tipg.link/gCuo> [fecha de consulta: 18.12.2023].
- Steinberg, Stacey (2017): «Sharenting: Children's privacy in the age of social media», en: *UF Law Scholarship Repository*, Vol. 66, N° 839: pp. 839-884.
- Véliz, Carissa (2020): «El desafío de la privacidad en la era tecnológica», en: Fàbregues, Francesc y Farrés, Oriol (editores), *Anuario internacional Cidob* (Barcelona, Nueva Época).
- Verswijvel, Karen y Ouvrein, Gaelle (2019): «Sharenting: Parental adoration or public humiliation? A focus group study on adolescents 'experiences with sharenting against the background of their own impression management», en: *Children and Youth Services Review*, Vol. 99: pp. 319-327: [DOI [10.1016/j.childyouth.2019.02.011](https://doi.org/10.1016/j.childyouth.2019.02.011)].

Jurisprudencia citada

Corte Constitucional de la República de Colombia, 1 de julio de 2022, sentencia T-245A/22 sobre el derecho al ambiente familiar sano e in-

terés superior de los niños, niñas y adolescentes; progenitores deben mantener rol de garantes, protectores y cuidadores de sus hijos, frente a la exposición de imágenes y videos en redes sociales.

- Organización de las Naciones Unidas, Asamblea General, 22 de febrero de 2021, La inteligencia artificial y la privacidad, así como la privacidad de los niños, en: informe del relator especial sobre el derecho a la privacidad, Joseph A. Cannataci, Consejo de Derechos Humanos, 46° periodo de sesiones, A/HRC/46/37.
- Organización de las Naciones Unidas, Asamblea General, 22 de febrero de 2021, documento del Organismo Nacional de Protección de Datos y Libertad de la Información de Hungría, en: La inteligencia artificial y la privacidad, así como la privacidad de los niños, informe del relator especial sobre el derecho a la privacidad, Joseph A. Cannataci, Consejo de Derechos Humanos, 46° periodo de sesiones, A/HRC/46/37.
- Organización de las Naciones Unidas, Asamblea General, 23 de julio de 2021, informe del relator especial sobre el derecho a la privacidad, Joseph A. Cannataci, 76° periodo de sesiones, A/76/220.
- United States, 24 de agosto de 2021, District Court II Central, District of California, *Spencer Elden vs Nirvana LLC*, -cv-06836.
- Tribunal De Justicia de la Unión Europea, Sentencia del Tribunal de Justicia (Gran Sala), asunto C-131/12, *Google Spain-Google Inc. y Agencia Española de Protección de Datos (AEPD) con Mario Costeja González* (13.05.2014).

Normativa citada

- Agencia Española de Protección de Datos, AEPD, Fichas de protección de datos y prevención de delitos. Disponible en: <https://tipg.link/g-20>.
- Comisión Europea, Estrategia de la UE sobre los Derechos del Niño (24.2.2021).
- Organización de los Estados Americanos, Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), Gaceta Oficial n. 9460 (22.II.1969).
- Organización de las Naciones Unidas, Asamblea General, Convención sobre los Derechos de los Niños (20.9.1989).
- Secretaría General Iberoamericana, Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, adoptada en la XXVIII Cumbre Iberoamericana de Jefes y Jefes de Estado y de Gobierno (25.3.2023).
- Unión Europea, Directiva 2002/58/ del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (12.7.2002).

Unión Europea, Directiva 2011/83/ del Parlamento Europeo y del Consejo sobre los derechos de los consumidores (25.10.2011).

Unión Europea, Directiva 2011/93/del Parlamento Europeo y del Consejo relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil (13.12.2011).

Unión Europea, Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (27.4.2016).

AGRADECIMIENTOS

La autora agradece especialmente a su director de tesis doctoral, doctor Johann Benfeld Escobar, por sus relevantes comentarios, observaciones y sugerencias al borrador de este artículo. Cualquier objeción que pudiera generarse a propósito de los resultados de esta investigación son atribuibles y de responsabilidad exclusiva de la autora. De igual modo, la autora agradece el acceso a los recursos físicos y electrónicos contenidos en el sistema de bibliotecas María Zambrano de la Universidad Complutense de Madrid, gracias al soporte logístico de la Sección Departamental de Derecho Constitucional de la Facultad de Ciencias de la Información.

FINANCIAMIENTO

Esta investigación cuenta con el apoyo de la Agencia Nacional de Investigación y Desarrollo (Anid-Conicyt), Chile, beca doctorado nacional 21220932.

SOBRE LA AUTORA

MARYORI MOLINA LUNA es magíster *scientiae* en Ciencias Políticas, abogada y politóloga por la Universidad de Los Andes, Venezuela. También es candidata a doctora en Derecho por la Pontificia Universidad Católica de Valparaíso y becaria Anid-Conicyt. Su correo electrónico es maryori.molina.l@mail.pucv.cl.  <http://orcid.org/0000-0002-4371-0518>.