

La protección de las niñas, niños y adolescentes y el principio de anonimato aplicado a la Sociedad de la Información y el Conocimiento. Una reflexión sobre la no-identificación funcional en el nuevo entorno tecnológico

*Gabriela Mendoza Correa**

Los beneficios que Internet brinda son evidentes, sin embargo debemos reflexionar también sobre los peligros e inconvenientes que representa, en particular si se trata de proteger y difundir los derechos e intereses de los más pequeños. La posibilidad de la participación anónima o el uso de pseudónimos en las redes sociales coadyuva en el respeto a la privacidad y a la dignidad de los usuarios, en un momento donde la telecomunicación incorpora diversos identificadores técnicos que permiten seguir el curso y rastrear nuestro comportamiento en la red. Este nuevo entorno tecnológico, precisa que alcancemos un punto de equilibrio entre el derecho a la libertad de expresión y el derecho al anonimato.

*La autora es Doctora en Antropología Social por la Universidad Complutense de Madrid, es Maestra en Política Internacional con especialidad en derechos humanos por la Universidad de Londres (School of Oriental and African Studies) y Licenciada en Relaciones Internacionales por la Universidad Iberoamericana. Se ha desempeñado como Coordinadora de Asesores en la Consejería Jurídica del Ejecutivo Federal así como en la Subsecretaría de Asuntos Jurídicos y Derechos Humanos de la Secretaría de Gobernación (México). Ha escrito y publicado varios artículos sobre derechos humanos, política internacional y migración, equidad de género, derecho a la privacidad y protección de datos. Actualmente, colabora en el Instituto Federal de Acceso a la Información y Protección de Datos de México.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

“En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño”.¹

Introducción

En la actualidad, podemos afirmar que Internet es un medio de comunicación de masas al que las niñas, niños y adolescentes acceden cada vez con más facilidad. Desde el inicio, Internet fue diseñada como una tecnología abierta, de libre uso, con el propósito deliberado de favorecer la libre comunicación global.

Los beneficios que Internet tiene para los niños y adolescentes son evidentes, principalmente me refiero a los que sirven como recurso educativo, los que les permiten mejorar sus conocimientos y acceder a la información, aquellos que facilitan la interacción con personas de todo el mundo, además de aprender compartiendo experiencias en el entorno tecnológico.

Sin embargo, conscientes de estos beneficios debemos reflexionar también sobre los peligros e inconvenientes que Internet presenta, en particular si se trata de proteger y difundir los derechos e intereses de los más pequeños. La posibilidad de la participación anónima o el uso de pseudónimos en las redes sociales digitales coadyuvan en el respeto a la privacidad y a la dignidad de los usuarios, en un momento donde la telecomunicación incorpora diversos identificadores técnicos que permiten seguir el curso y rastrear nuestro comportamiento en la red.

En este sentido, el acelerado avance tecnológico ha desarrollado una aproximación genérica al estudio de las regulaciones sobre la protección de datos, de tal forma que en la actualidad irrumpe en la metodología una tercera generación que proporciona un nivel adicional de protección, manteniendo inalteradas las medidas antes introducidas.

¹Véase Artículo 3 relativo al *interés superior del niño* de la Convención sobre los derechos del niño adoptada el 20 de noviembre de 1989 y disponible en el vínculo siguiente: <http://www2.ohchr.org/spanish/law/crc.htm>

GABRIELA MENDOZA CORREA

Recordemos que la primera generación se enfocaba en la naturaleza de los datos, en particular en aquella información de carácter sensible y su efecto sobre el dominio privado de los individuos, viéndose plasmada en el artículo 8 del *Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales* que hace referencia al derecho a la vida privada, de tal forma que la autodeterminación informativa fue entonces equiparada con la prohibición de procesamiento de información sensible.²

Es decir, esta disposición legal protege la esfera privada del individuo garantizando el respeto a la vida privada, a la vida familiar, al domicilio y a la correspondencia, reconociendo cuatro ámbitos diferentes de protección. Estos ámbitos forman una unidad, una ‘esfera privada’ del individuo, indispensable para el libre desarrollo de la personalidad.

Por su parte, la segunda generación avanza enfocándose en el tratamiento de los datos y en el equilibrio de poder entre los procesadores de información y los sujetos de ese tratamiento dando origen a la *Convención No. 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* que garantiza la transparencia en el procesamiento de la información y restringe el derecho al manejo de datos sobre terceros.³

En consecuencia, la tercera generación reconoce la tecnología en sí misma por su potencial multiplicador, en virtud que la tecnología incrementa la cantidad de datos y de individuos con acceso a ellos y por tanto, el poder de recopilar y procesar más allá de las fronteras. En esta nueva generación, subyace la importancia de la terminal o la red como nueva variable en la ecuación, que interviene

²Cabe subrayar que el texto de este artículo está inspirado en el artículo 12 de la *Declaración Universal de los Derechos Humanos* y en el artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos* que en su conjunto reconocen el derecho al respeto a la vida privada y familiar satisfaciendo la necesidad de un ámbito propio y reservado de los individuos. El *Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales* está disponible para su consulta en el vínculo electrónico siguiente: <http://www.echr.coe.int/Library/COLEncedh.html>

³La *Convención No. 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* está disponible en el vínculo electrónico siguiente: <http://conventions.coe.int/treaty/en/treaties/html/108.htm>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

ahora entre el individuo y el controlador de datos, de forma tal que la autodeterminación informativa demanda mecanismos de control sobre esta nueva variable.

Es así como, mientras somos testigos del desarrollo tecnológico como característica esencial de nuestra sociedad surge la necesidad de una protección más amplia de los derechos en el nuevo contexto social, en donde la universalización del acceso a la tecnología, la libertad de expresión en el Internet y la libre circulación de los datos juegan un papel fundamental al tiempo que reclaman reflexiones en torno a la protección de la información.

A este respecto, es preciso señalar que la protección de la información no representa un impedimento para la libre circulación, por el contrario, en la actualidad el titular cuenta con facultades para dar o no su consentimiento para el tratamiento de sus datos, para conocer que su información personal está siendo tratada y los propósitos o motivos de dicho tratamiento, o bien, para acceder, rectificar o cancelar los datos en un momento posterior.

Ahora bien, en lo que respecta a las niñas, niños y adolescentes son varios los instrumentos internacionales que garantizan su protección en el ámbito de la Sociedad de la Información y el Conocimiento. Sobre el particular, dos son los textos fundamentales que regulan el tema de su protección en la interacción con el Internet, ambos en el ámbito europeo.

En primera instancia la “Decisión del Consejo de la Unión Europea del 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet”, propone medidas para intensificar la colaboración entre los Estados miembros independientemente de que cada uno de ellos aplique la legislación que exista en su país sobre la materia. De esta forma determina que los Estados miembros “establecerán la cooperación más amplia y rápida posible para facilitar una investigación y persecución eficaces de los hechos punibles relativos a la pornografía infantil en Internet, con arreglo a los acuerdos y disposiciones vigentes”.⁴

⁴Este documento se fundamenta a su vez en la *Resolución del 27 de febrero de 1996 del Consejo de Telecomunicaciones para impedir la difusión de contenidos ilícitos de Internet, especialmente la pornografía infantil*, el *Convenio Europeo para la Protección*

GABRIELA MENDOZA CORREA

Por otra parte, destaca el “Libro Verde sobre la Protección de Menores y de la Dignidad en los Servicios Audiovisuales y de Información”, cuyo objetivo es crear un marco adecuado de protección de los niños y adolescentes en los servicios audiovisuales y de información en la Unión Europea. Establece que para el desarrollo de las nuevas tecnologías hay que utilizar medios rápidos y eficaces que acaben con los contenidos que atentan a la dignidad de las personas, especialmente del colectivo que aquí nos concierne.⁵

En la primera parte, plantea la necesidad de diferenciar entre los contenidos que son ilícitos, que están sujetos a sanciones penales —como la pornografía infantil— y por lo tanto no deben tener cabida en la red y el hecho de que los niños y adolescentes puedan a acceder a páginas pornográficas que no son ilegales para adultos.

El Capítulo II precisa que las disposiciones aplicables a nivel nacional y europeo se inscriben en el marco de los derechos fundamentales que figuran en el *Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales*,⁶ en particular en el artículo 10 que proclama la libertad de expresión, estableciendo que la misma puede verse limitada para evitar la prevención de delitos.

De la misma manera, la libre prestación de servicios, que constituye una de las cuatro libertades que garantiza el *Tratado de la Unión Europea*, puede verse restringida por razones primordiales de interés público, como la protección de los niños y adolescentes, así como de la dignidad humana. Se plantean también diferentes posibilidades para reforzar la cooperación entre las diferentes administraciones nacionales: intercambio de informaciones, análisis normativo comparado, cooperación en los marcos de la justicia y de los asuntos interiores, entre otros.

de los Derechos Humanos y de las Libertades Fundamentales y la Declaración Universal de los Derechos Humanos, así como otros documentos relativos a la protección de los derechos humanos y los derechos de la infancia. La “Decisión del Consejo de la Unión Europea del 29 de mayo de 2000”, puede consultarse en el Diario Oficial no. L 138 de 09/06/2000 pp.0001-0004, o bien en el vínculo electrónico siguiente: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0375:ES:HTML>

⁵Disponible para su consulta en el vínculo electrónico siguiente: http://europa.eu/legislation_summaries/audiovisual_and_media/l24030_es.htm

⁶Disponible en el vínculo siguiente: http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

En suma, existe un amplio abanico de instrumentos jurídicos internacionales, primordialmente europeos, que tienen como objetivo la protección de las niñas, niños y adolescentes en su interacción con las tecnologías del conocimiento y la información. En el ámbito latinoamericano las iniciativas en esta dirección destacan lo establecido por el “Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes”,⁷ suscrito el 28 de julio de 2009 en Montevideo —de ahí que es referido comúnmente como *Memorándum de Montevideo*— en el Seminario Derechos, Adolescentes y Redes Sociales en Internet. El texto refiere la participación anónima y al uso de seudónimos de la forma siguiente:

3.1. *La participación anónima o el uso de pseudónimos es posible en las redes sociales digitales.* El proceso educativo debe reflexionar sobre los aspectos positivos del uso de pseudónimos como medio de protección y un uso responsable que —entre otras cosas— implica no utilizarlos para engañar o confundir a otros sobre su identificación real. Las niñas, niños y adolescentes deben ser advertidos sobre la posibilidad de que cuando creen estar comunicándose o compartiendo información con una persona determinada, en realidad puede tratarse de otra persona. Al mismo tiempo es necesario advertir que la participación anónima o con un pseudónimo hace posible la suplantación de identidad.⁸

En efecto, existen leyes y normatividad en la materia que defiende el derecho al anonimato, sin embargo es razonable cuestionarnos sobre la efectividad real de ese derecho. Lo anterior, en virtud de que las terminales de telecomunicación incorporan diversos identificadores técnicos que permiten el rastreo y la construcción de perfiles de acuerdo al comportamiento de los individuos en la red. El problema radica en que la gran mayoría de la industria no considera al proceso de rastreo como una violación de la privacidad de las personas, al no poder ser identificados mediante un punto de contacto.⁹ Más aun, los protocolos de telecomunicaciones y el funcionamiento de los terminales no incluyen la protección de da-

⁷El texto íntegro del *Memorándum de Montevideo* está disponible en la versión en español en el vínculo siguiente: <http://memorandumdemontevideo.ifai.org.mx/>

⁸*Ibid.* En la sección sobre “Recomendaciones para los Estados y Entidades Educativas para la Prevención y Educación de niñas, niños y adolescentes”. [Énfasis añadido].

GABRIELA MENDOZA CORREA

tos como requisito fundamental, sino como una opción más puesta a discreción de la industria fabricante de dispositivos y programas.

En consecuencia, la idea de ‘anonimizadores’ se ha venido desarrollando, y en la actualidad existen numerosas empresas que permiten utilizar la red sin dejar huella, y por ello generan ganancias económicas, antes inimaginables, generando así un extendido mercado de encriptación y anonimato.¹⁰

En suma, el anonimato tiene consecuencias tanto positivas como negativas. Por una parte, hay quien subraya su contribución a las libertades. Por otro lado, otros se enfocan en las víctimas de acciones delictivas producto del anonimato, y concluyen que por lo menos, algunas formas de anonimato deberían estar prohibidas.

El argumento de los detractores del anonimato es simple. Arguyen que el anonimato es un acto deshonesto porque facilita el hacer el ‘mal’ eliminando el sentido de la responsabilidad, siendo esta comúnmente el propósito fundamental del anonimato.¹¹ Sin embargo, el anonimato podría ser el único mecanismo disponible para el común de las personas que les defienda —aunque de forma parcial— contra la elaboración de perfiles y el rastreo en las comunicaciones.

El debate inconcluso sobre la legalidad y la moralidad de las comunicaciones anónimas puede ser entendido dentro de un marco más amplio en donde se cuestiona el grado de alcance de los individuos y el control que tienen sobre la difusión de su información. Un debate que se refleja por un lado en leyes de protección de datos más firmes, y por otro en las demandas del mercado en manos de buros de crédito y de despachos de minería de datos, así como el creciente uso por parte de los gobiernos de las bases de datos, de perfiles y de técnicas de autorización de seguridad.

⁹La tecnología de los *cookies* permite que una página web, por defecto y automáticamente, inserte su propio identificador de forma permanente para poder así rastrear el comportamiento del individuo en la red.

¹⁰De las cuales sobresale en la industria la canadiense *Zero Knowledge Systems* fundada en 1997 y disponible en el vínculo electrónico siguiente: <http://www.zeroknowledge.com/>

¹¹Michael Froomkin, “Anonymity in the Balance”, en C. Nicoll, J.E. Prins y M.J. van Dellen (eds.), *Digital Anonymity: Tensions and Dimensions*, Cambridge University Press, Cambridge, 2003. Asimismo, en “The Dead of Privacy”, *Stanford Law Review*, Vol. 52, Stanford University, 2000, pp. 1461-1563.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Es en este amplio escenario donde se enclava la cuestión sobre la dualidad entre anonimato y libertad de expresión, ambos derechos de todos los individuos, adquiriendo especial relevancia al ser aplicados a las niñas, niños y adolescentes.

1. Sobre los nuevos principios para la promoción de la autodeterminación informativa en el nuevo entorno tecnológico. El principio de encriptación y anonimato reversible

“[...] si la red es global, el acceso es local, a través de un servidor. Y es en este punto de contacto entre cada ordenador y la red global en donde se produce el control más directo”.¹²

Con la abolición de fronteras nacionales emerge la necesidad de hacer un frente común a la protección de datos y su posible implementación más allá de las fronteras nacionales. De tal manera que para contrarrestar los riesgos ante este nuevo contexto, se han venido esbozando a manera de un primer intento, principios para la mejor protección y el mayor control en el entorno tecnológico.

Estos principios han sido desarrollados por Yves Poullet en colaboración con Jean-Marc Dinant, ambos catedráticos de la Universidad de Namur, y se han presentado a manera de reporte ante el Comité Consultivo del Convenio para la protección de individuos con respecto al proceso automático de datos personales (en adelante, “Convenio No. 108”) el 13 de diciembre de 2004 en Estrasburgo. El “Reporte sobre la aplicación de los principios de protección de datos en la Red Mundial de Telecomunicaciones” retoma los planeamientos del Convenio No. 108 sobre la autodeterminación informativa en el nuevo contexto de Internet.¹³

¹²Véase lección inaugural “Internet, libertad y sociedad: una perspectiva analítica” del curso académico 2000-2001 de la *Universitat Oberta de Catalunya* y pronunciado por el profesor Manuel Castells, catedrático del Instituto Interdisciplinario de Internet de la misma universidad. Disponible en el vínculo siguiente: http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html

¹³Véase para su consulta el vínculo electrónico siguiente: <http://www.coe.int/t/dghl/>

GABRIELA MENDOZA CORREA

Los autores esbozan cinco nuevos principios relacionados con la protección de los datos personales y el control de la privacidad, a saber:

- *El principio de encriptación y anonimato reversible.*
- El principio de beneficios recíprocos.
- El principio al fomento de aproximaciones tecnológicas compatibles con la situación de personas protegidas legalmente o su mejora.
- El principio de que el usuario mantenga pleno control sobre el equipamiento terminal.
- El principio de que los usuarios de determinados sistemas de información deberían beneficiarse de la legislación de protección al consumidor.

El primer principio sobre encriptación y anonimato reversible nos concierne en particular. El concepto de encriptación es mucho más claro que el de anonimato, dado que ofrece protección contra el acceso a contenidos en las comunicaciones y su calidad varía de acuerdo a las técnicas aplicadas. En el mercado actual, podemos encontrar programas de encriptación a precios asequibles y de relativa facilidad para los usuarios.

Por su parte, el concepto de anonimato no es tan nítido dada su ambigüedad, al punto que muchos académicos proponen que el término sea sustituido por otros como ‘no-identificable’, o bien ‘pseudoanonimato’. La confusión del término radica en que no siempre se busca el anonimato absoluto, sino la “no-identificación funcional del autor de un mensaje enviado a otras personas”,¹⁴ de ahí que las distinciones entre grados de anonimato resultan importantes en virtud de las implicaciones legales.

Por tanto, el principio sobre anonimato se ha transformado en un derecho que se ha plasmado en distintos documentos interna-

standardsetting/dataprotection/TPD%20documents/T-PD%20_2004_%2004%20E%20final%20Report%20POULLET.pdf

¹⁴A mayor abundamiento en los grados de anonimato tecnológico en transferencias electrónicas puede consultarse el artículo de J. Grijpink y C. Prins.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

cionales no vinculantes, entre los que destaca la *Recomendación 3/97 de 3 de diciembre de 1997 sobre el anonimato en Internet*,¹⁵ adoptada por el Grupo de Trabajo del Artículo 29 sobre Protección de las personas en lo que respecta al tratamiento de datos personales, y fundamentado en el “Memorándum de Budapest-Berlín sobre protección de datos e intimidad en Internet”.¹⁶ También sobresale la *Recomendación No. R (99) 5 del Comité de Ministros del Consejo de Europa* que puntualiza que “el acceso anónimo para el uso de servicios, y medios anónimos para realizar pagos son la mejor protección a la privacidad”.¹⁷ De esta forma, la creciente aparición de instrumentos internacionales con estas características subraya no solo la importancia de salvaguardar la privacidad y motiva la aparición de tecnologías en el mercado, además propugna por el reconocimiento del ‘derecho al anonimato’ en el uso de servicios tecnológicos, en particular cuando existen transferencias monetarias.

De tal forma que el principio a la no-identificación funcional se expresa como derecho de la forma siguiente:

[...] Aquellos que usen técnicas modernas de comunicación deben *poder permanecer no identificados por los proveedores de servicios, por otras terceras partes que intervinieran durante la transmisión del mensaje y por el receptor o receptores del mensaje*, y deberían tener acceso gratis, o a precios razonables, a los medios de ejercitar esta opción. La disponibilidad de encriptación económica y herramientas y servicios para mantener el anonimato es una condición necesaria para internautas que ejerzan su responsabilidad personal.¹⁸

“New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity”, *Computer Law & Security Report*, The University of Warwick, Vol. 17, No. 6, 2001, pp. 379-389, citado en Y. Poulet, “Hacia nuevos principios de protección de datos en un nuevo entorno TIC”, *Revista d’Internet, Dret i Política*, Universitat Oberta de Catalunya, No. 5, 2007, p.37.

¹⁵Disponible para su consulta en el vínculo electrónico siguiente: <http://www.informatica-juridica.com/anexos/anexo476.asp>

¹⁶Disponible en el vínculo electrónico siguiente: <http://www.informatica-juridica.com/anexos/anexo508.asp>

¹⁷Véase el “Reporte sobre la aplicación de los principios de protección de datos en la Red Mundial de Telecomunicaciones”, p. 49. Disponible en el vínculo electrónico siguiente: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD%20_2004_%2004%20E%20final%20Report%20POULLET.pdf

¹⁸Y. Poulet, “Hacia nuevos principios... *Op.cit.*, p. 37. [Énfasis añadido].

GABRIELA MENDOZA CORREA

Asimismo, la Agencia Española de Protección de Datos emitió la *Resolución sobre Protección de la Privacidad en los servicios de redes sociales*, producto de la 30 Conferencia Internacional de Protección de Datos y Privacidad celebrada en Estrasburgo del 15-17 de octubre de 2008, donde se establece a la letra lo siguiente:

8. Uso del servicio bajo seudónimo.

Los proveedores deberán permitir la creación y utilización de perfiles seudónimos de forma opcional, y fomentar el uso de dicha opción.¹⁹

Sin embargo, el derecho al anonimato no siempre es absoluto en tanto que existan intereses superiores por parte del Estado, los cuales podrían restringir el ejercicio de este derecho.²⁰ Más aun, la cuestión radica en cómo lograr el equilibrio entre la protección de datos y la monitorización legítima de delitos. Los expertos señalan que es posible mediante el uso de ‘pseudo-identidades’ que podrían ser asignadas a individuos mediante proveedores de servicios especializados que, dado el caso, podrían ser requeridos para revelar la identidad real de un usuario en determinadas circunstancias y siguiendo procedimientos establecidos por la ley.

Los instrumentos internacionales en la materia,²¹ señalan en lo general dos mecanismos que permiten mantener el anonimato en cierta medida y que coadyuvan a garantizar la intimidad de las personas:

¹⁹Disponible en el vínculo electrónico siguiente: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf

²⁰En estudios de derecho comparado se han establecido como limitantes de este derecho a la acción estatal para proteger la seguridad nacional, defensa, seguridad pública y para la prevención, investigación, detección y persecución de delitos. A manera de caso ilustrativo, podemos citar el artículo 4 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* de México, que establece a la letra:

Artículo 4.- Los principios y derechos previstos en esta Ley, tendrán como límite en cuanto a su observancia y ejercicio, la protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros.

Disponible para su consulta en el vínculo electrónico siguiente: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

²¹En particular consultar la “Recomendación” 3/97... *Op.cit.*, p.7.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

- Servicios de reexpedición anónima (*remailers*). El proveedor de acceso puede ofrecer esta opción, o bien puede dirigir los mensajes a un servicio específico que garantiza el anonimato, que los reexpide de forma anónima.²²

- Acceso anónimo a la red. Puede accederse a la red de forma anónima, pagando por adelantado. Los servicios de reexpedición anónima implican el mantenimiento de un nexo entre el remitente del mensaje y el propio mensaje, vínculo que podría ser reconstruido con posterioridad –por ejemplo, con motivo de una investigación policial.

A este respecto, los académicos y en particular Michael Froomkin investigador destacado de la Universidad de Miami y experto en temas de privacidad y criptología, ha distinguido cuatro tipos de comunicación electrónica, donde la identidad física o ‘real’ puede ser parcialmente oculta, a saber:²³

- Anonimato rastreable. El servicio de reexpedición o *remailer*, no muestra datos de identificación del remitente, pero deja esta información en manos de un solo vínculo trazado el camino para la reconstrucción de un sistema anónimo rastreable.

- Anonimato no-rastreable. Es la forma de comunicación en la que el autor sencillamente no es posible de identificar. En la actualidad, la tecnología de Internet permite esta forma de anonimato mediante el enrutamiento de mensajes a través de una serie de *remailers* anónimos y es mejor conocida como ‘*remailers* en cadena’. Esta técnica abre la puerta al lado más

²²En la reexpedición anónima, un servidor de correo electrónico especial, recibe un mensaje de correo que incluye determinadas líneas que le indican lo que ha de hacer con ese mensaje. El *remailer* toma el mensaje, borra todo rastro de las cabeceras del mensaje que puedan identificar al remitente (como el campo *From:*) y lo reenvía a su destino real. El destinatario recibirá un mensaje sin identificación del remitente.

²³A mayor abundamiento, véase Michael Froomkin, “Anonymity and Its Enmities”, *Journal of Online Law*, University of Miami, 1995. Disponible en el vínculo electrónico siguiente: http://articles.umlau.net/froomkin/Anonymity_Enmities.htm

Asimismo, en Michael Froomkin, “Anonymity in the Balance”, en C. Nicoll, J.E. Prins y M.J. van Dellen (eds.), *Digital Anonymity...* Op. cit. Disponible en el vínculo siguiente: <http://osaka.law.miami.edu/~froomkin/articles/balance.pdf>

GABRIELA MENDOZA CORREA

oscuro de la comunicación no rastreable, haciendo del anonimato una herramienta eficaz para evadir la detección de actividades ilegales.

- Pseudónimos rastreables. Esta técnica de comunicación cuenta con un *nom de plume* adjunto que puede ser rastreado hasta el autor original del mensaje —que no necesariamente es el remitente con identificación real, sino su pseudónimo.

- Pseudónimos no-rastreables. Trabaja de forma similar al anonimato rastreable, excepto que el usuario remitente utiliza un pseudónimo (*nym*).

El principio de anonimato en cualquiera de sus formas está vinculado naturalmente con el derecho a la protección de datos. Este derecho se entiende como el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso. También se le conoce como el derecho a la ‘autodeterminación informativa’ que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaban, manejar y utilizan sus datos personales.

El derecho a la protección de datos personales como se concibe en la actualidad, también deviene de una transformación, desde la concepción del derecho a la vida privada y la intimidad, hasta la conformación de un nuevo derecho fundamental dotado de caracteres propios, que otorgan a la persona un haz de facultades concretas. Por tanto, se trata en sí mismo de un derecho activo.²⁴

Ahora bien, las implicaciones del anonimato tecnológico conllevan la regulación de los equipamientos terminales con el objeto de prevenir la monitorización de la navegación, para permitir la creación de direcciones efímeras y para la diferenciación de datos de direcciones para el acceso exclusivo de terceras personas autorizadas, y para la desaparición de los identificadores únicos globales mediante la introducción de protocolos de direcciones uniformes.

En este sentido, se ha sugerido la creación de requisitos mínimos para los servicios proporcionados y con respecto a la protección

²⁴Pablo Murillo de la Cueva, y José Luis Piñar Mañas, *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009.

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

del dato, que deberán de ser aprobados de forma oficial, similar a lo que se hace con las firmas digitales o las etiquetas de calidad.

La *Recomendación 3/97* antes mencionada, aporta en este sentido conclusiones operativas en los contextos normativo, tecnológico y económico además de la sensibilización a usuarios y proveedores de Internet.

RESUMEN DE LAS PRINCIPALES CONCLUSIONES DE LA RECOMENDACIÓN 3/97²⁵

- La posibilidad de mantener el anonimato es fundamental para que la intimidad de las personas goce de la misma protección en línea que fuera de línea.
- La posibilidad de anonimato no siempre resulta oportuna. A la hora de determinar en qué circunstancias lo es y en cuáles no, deben contrapesarse cuidadosamente los derechos fundamentales a la intimidad y a la libertad de expresión con otros objetivos importantes de orden público, entre ellos la prevención de la delincuencia. Las restricciones legales que puedan imponer los Gobiernos al derecho de mantener el anonimato o a los medios técnicos utilizados al efecto (p. ej., disponibilidad de productos de codificación) deberán en todo momento ser proporcionadas y limitarse a lo estrictamente necesario para proteger un interés general específico en una sociedad democrática.
- En la medida de lo posible, el equilibrio alcanzado en relación con tecnologías anteriores deberá preservarse en lo que respecta a los servicios ofrecidos a través de Internet.
- Deberá ser posible mantener el anonimato a la hora de enviar correo electrónico, navegar pasivamente por emplazamientos de la World Wide Web y adquirir la mayor parte de bienes y servicios a través de Internet.
- Aun cuando sean necesarios ciertos controles de los particulares que envían colaboraciones a los foros públicos en línea (grupos de debate, etc.), la exigencia de identificación de las personas resulta a menudo desproporcionada e inviable, por lo que debería optarse por otras soluciones.

²⁵ *Ibid.*, p. 13

GABRIELA MENDOZA CORREA

-
- Los medios anónimos de acceso a Internet (p. ej., kioscos públicos Internet, tarjetas de acceso prepagadas) y los medios anónimos de pago constituyen dos elementos esenciales con vistas al verdadero anonimato en línea.
-

En cuanto al ámbito normativo se señala que la obtención de datos personales deberá limitarse al mínimo necesario y deberá reconocerse en las normas domésticas e internacionales en la materia, además de incorporarse en códigos de conducta, directrices y demás documentos reguladores no legislativos.²⁶ Destaca que “deberá preverse el derecho de las personas a mantener, si lo desean, el anonimato”.²⁷

En el contexto tecnológico, señala que deberá fomentarse el debate para desarrollar una infraestructura y protocolos de Internet que favorezca la actividad anónima de los usuarios. Por su parte, en el contexto económico, sugiere que las administraciones “deberán estudiar la manera de ofrecer apoyo económico que impulse la adopción generalizada en el mercado de tecnologías que favorezcan la intimidad y permitan a las personas mantener el anonimato”.²⁸

Finalmente, la sensibilización de los usuarios de Internet, los proveedores de acceso y servicios y el sector de las tecnologías de la información en general deberán ser concientizados de la importancia del derecho a la privacidad a través de consejos y orientaciones por parte de las autoridades responsables a la protección de datos, coadyuvando así a la construcción de una cultura en esta materia y en íntimo balance con el derecho a la libertad de expresión.

²⁶Los “Estándares Internacionales sobre Protección de Datos Personales y Privacidad” (mejor referidos como *Estándares de Madrid*), presentados en la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, se refiere al principio de proporcionalidad como “el tratamiento de datos de carácter personal [que] deberá circunscribirse a aquellos que resulten adecuados, relevantes y no excesivos en relación con las finalidades previstas en el apartado anterior. En particular, la persona responsable deberá realizar esfuerzos razonables para limitar los datos de carácter personal tratados al mínimo necesario”. Documento disponible en el vínculo siguiente: https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/com-mon/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

²⁷“Recomendación 3/97... *Op. cit.*, p. 13.

²⁸*Ídem.*

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

2. El significado social del anonimato en Internet

“¿Cómo dejar fuera del análisis ese vasto pedazo de lo real que es lo virtual?”²⁹

Continuos debates sobre la privacidad digital estimulan la discusión sobre las maneras plausibles para evitar ser identificado en la red y poder comunicarnos de forma anónima. Es así como las comunicaciones anónimas emergen con vital importancia en el discurso social y político.

Como hemos visto, la comunicación anónima tiene innumerables implicaciones en varios ámbitos, y ha adquirido importancia en la medida en que aumenta el deseo de los usuarios de permanecer anónimos. Una de las razones de este incremento radica en la preocupación sobre la privacidad en la era digital, de tal forma que el tema de la protección a la privacidad se aborda desde el anonimato con el propósito de salvaguardar el derecho de la libertad de expresión. Ahora bien, debido al carácter internacional de la red, las razones relacionadas con la libertad de expresión y las comunicaciones anónimas adquieren una nueva dimensión, en particular en lo referente a la actividad criminal.

Esto es, los cambios que el Internet ha traído son de gran alcance, pero inevitablemente conllevan nuevos problemas y presentan nuevos retos a quienes definen y desarrollan normas de orden público y velan por su cumplimiento, donde especial matiz adquieren la normativa en este ámbito abocada a la protección de la niñez, pues es imprescindible que ellos entiendan que lo que es ilícito fuera de línea lo es también en la red.

En todos los ámbitos se discuten nuevas ideas y proponen posibles soluciones orientadas a asegurar los intereses sociales frente a los avances tecnológicos en lo que nos concierne, me refiero aquí al interés superior del niño. Empero, un problema común radica en la dificultad de detectar actividades ilícitas en un ámbito donde se complica la identificación de la persona responsable. Esto no quiere

²⁹Néstor García Canclini, *Diferentes, desiguales y desconectados. Mapas de la Interculturalidad*, Gedisa Editorial, Barcelona, 2004, p. 151.

GABRIELA MENDOZA CORREA

decir que el derecho a la libertad de expresión se contraponga con el derecho a la privacidad necesariamente, sin embargo se necesita conciliar la intimidad con otros objetivos de orden público, por lo que es importante alcanzar el equilibrio entre participar en la red de forma anónima y sentar los límites de dicha interacción.

Ahora bien, una de las mayores amenazas al derecho a la privacidad es la capacidad que tienen algunas empresas y organizaciones de acumular gran cantidad de datos electrónicos sobre particulares que hacen posible su tratamiento, alteración y transmisión con rapidez y a un bajo coste. La amenaza a vulnerar el derecho a la privacidad no se deriva exclusivamente de la cantidad de datos personales en Internet, sino en el desarrollo de soportes lógicos capaces de buscar en la red y recopilar la información sobre una persona y generar así un perfil específico.

Es precisamente en este contexto en el que se enclava la evolución normativa hacia un uso adecuado de las tecnologías de la información y lo que ha motivado a los Estados miembros de la Unión Europea a adoptar disposiciones relativas a la protección de datos.³⁰ Por tanto, “la pretensión de anonimato en las comunicaciones en línea se considera ya plenamente legítima en determinadas situaciones”.³¹

Un caso que sentó precedentes a este respecto es el relativo a *McIntyre v. Ohio* (1995) en los Estados Unidos de Norteamérica. En 1998, Margaret McIntyre distribuyó panfletos afuera de la

³⁰En el contexto europeo, tal ha sido el caso de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, *relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, asimismo la Directiva 2002/58/CE del Parlamento Europeo y del Consejo del 12 de julio de 2002, *relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas* (Directiva sobre la privacidad y las comunicaciones electrónicas) [Diario Oficial L 201 de 31.7.2002]. Ambas disponibles en el vínculo electrónico siguiente: http://europa.eu/legislation_summaries/information_society/l14012_es.htm

Por su parte en el contexto latinoamericano, varios han sido los países que cuentan con legislación en la materia, México, Chile, Argentina y Uruguay por citar algunos.

³¹Por ejemplo, cuando una persona que es víctima de un delito sexual o padece dependencia a las drogas o al alcohol y quiere compartir su experiencia en la red de forma anónima sin riesgo de ser identificado. Para otros ejemplos ilustrativos, véase *Recomendación 3/97... Op. cit.*

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Blendon Middle School en Westernville, Ohio, oponiéndose al incremento del impuesto escolar –mismo que requería la aprobación mediante referéndum-. Los panfletos violaban el Código de Ohio que establecía que cualquier publicación general que tuviera como objeto afectar una elección o promover la adopción o erradicación de cualquier punto que pudiera influenciar a los votantes debería contener el nombre y la dirección de la persona responsable de la publicación. En consecuencia, se le adjudicó una multa de \$100 dls., lo que desató que se apelara a la Suprema Corte de Justicia de los Estados Unidos.³² En 1995, esta corte se pronunció sobre la cuestión, argumentando que el derecho a la libre expresión anónima está protegido por la Primera Enmienda, y explica:

La protección para la expresión anónima es vital para el discurso democrático. Permitiendo que los disidentes protejan su identidad los libera para expresarse críticamente, perspectivas minoritarias [...] El anonimato es el escudo contra la tiranía de la mayoría [...] De esta forma se ejemplifica el propósito detrás de la Carta de los Derechos Fundamentales, y en particular de la Primera Enmienda: para proteger individuos poco populares de las represalias [...] en manos de una sociedad intolerante.³³

Ahora bien, cabe destacar un caso significativo posterior en esta materia, me refiero al caso *Dendrite International, Inc. v. John Doe, No. 3* donde una corte de apelaciones del estado de Nueva Jersey en los Estados Unidos estableció que en la mayoría de los casos los avisos de información electrónica podrán mantener anónima la identidad de quien anuncia, y motivó a promulgar reglas para proteger sus intereses.³⁴

³²A mayor abundamiento puede consultarse el artículo de Michael Froomkin, "Anonymity in the Balance", en C. Nicoll, J.E. Prins y M.J. van Dellen (eds.), *Digital Anonymity...* Op.cit. pp. 12-17.

³³*McIntyre v. Ohio* (1995) (trad. propia). La decisión de la Suprema Corte de los Estados Unidos de Norteamérica respecto de este caso puede ser consultada para mas detalles en el vinculo electrónico siguiente: <http://www.law.cornell.edu/supct/html/93-986.ZO.html>

Asimismo, existen otros casos relevantes como el de *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964), así como el de *NAACP v. Alabama ex. Rel. Patterson*, 357 U.S. 449 (1958).

³⁴A mayor abundamiento sobre el caso *Dendrite International Inc. v. John Doe No. 3*, 775 A.2d 756, 760 (N.J. Super, 2001) véase Michael Froomkin, "Anonymity and Its Enmities", *Journal of Online...* Op. cit.

GABRIELA MENDOZA CORREA

Estos son antecedentes simbólicos para el anonimato en la red, ya que la protección del derecho al anonimato en el ámbito de la Sociedad de la Información y el Conocimiento es de vital importancia, debido a que el Internet ofrece un foro democrático y poderoso para la libertad de expresión.

3. Vinculación del derecho al anonimato con el ambiente de los niños y las TICs

Las niñas, niños y adolescentes figuran entre los usuarios más prolíficos de Internet y los aparatos móviles. Al navegar por el ciberespacio en busca de información y diversión y, acceder a redes sociales, también resultan ser los más expuestos al abuso.

En los últimos tiempos, los servicios de redes sociales particularmente han experimentado un gran auge entre el público infantil.³⁵ Entre otras cosas, estos servicios ofrecen medios de interacción basados en perfiles personales que generan sus propios usuarios, lo que ha propiciado un nivel sin precedentes de divulgación de información de carácter personal de los usuarios.

Ahora bien, la utilización de estos servicios puede plantear riesgos para la privacidad de los usuarios y de terceras personas ya que los datos personales relativos a las personas son accesibles de forma pública y global, de una manera y en unas cantidades sin precedentes -incluidas enormes cantidades de fotografías y video digitales.

Asimismo véase Michael Froomkin, “The Dead of Privacy”, *Stanford Law Review*, Vol. 52, Stanford University, 2000, pp. 1461-1563. Disponible en el vínculo electrónico siguiente: <http://osaka.law.miami.edu/~froomkin/articles/privacy-dead-thof.pdf>

³⁵El servicio de redes sociales ha sido definido por el Grupo de Trabajo de Protección de Datos (Artículo 29), como las “plataformas de comunicación en línea que facilitan a los individuos a crear o unirse a una red con usuarios de ideología afín. En el sentido legal, las redes sociales son servicios sociales de información, como se definen en el artículo 1, párrafo 2 de la Directiva 98/34/EC y reformada por la Directiva 98/48/EC”. Véase Opinión 5/2009 sobre redes sociales en línea del Grupo de Trabajo de Protección de Datos de la Comisión Europea, p. 4. Disponible en el vínculo siguiente: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Conscientes de los riesgos potenciales de los niños y adolescentes al interactuar en Internet, en América Latina y el Caribe así como en otras regiones, se están realizando valiosos esfuerzos para establecer un equilibrio entre la garantía de los derechos de acceso a la Sociedad de la Información y el Conocimiento y la protección ante los riesgos inherentes al uso de tecnologías de la información, a través del anonimato y otros mecanismos de interacción. De ahí el lanzamiento en la región del *Memorándum de Montevideo* el 3 de diciembre de 2008 en la Ciudad de México.³⁶

Tomando en consideración que el ciberespacio como entorno virtual ha transformado las variables de espacio y de tiempo, de modo que hoy en día existe la posibilidad de comunicarse casi instantáneamente con otra persona que puede encontrarse en el otro extremo del mundo, sin que la distancia física sea un problema. Esta transformación de las realidades hace que todo funcione más deprisa, provocando una alteración de la sociedad y por ende, de la familia y de la escuela.

Ahora bien, en lo que respecta a la protección del niño en particular, esta idea no es añeja, en tanto que es a finales del siglo XX cuando se reconoce a éste como sujeto de derechos. Aunado al hecho que, es en tiempos relativamente recientes que evoluciona la sociedad de la información y se precisa la protección del niño en este ámbito. Esta evolución de derechos nos lleva a establecer que la niñez, en cualquier parte del mundo, tienen el derecho a un medio ambiente seguro, inclusive en el espacio virtual.

Desde los años noventa, hemos podido ser testigos del creciente desarrollo de la red informática global, en los últimos diez años se ha disparado el número de aulas que cuentan con equipos informáticos conectados a Internet. Este avance hizo que florecieran nuevas formas de criminalidad hasta ese momento desconocidas. Ello ha motivado que en los ámbitos doméstico e internacional se hayan buscado soluciones para salvaguardar la seguridad de las niñas, niños y adolescentes que acceden a Internet.

³⁶En México, el Instituto Federal de Acceso a la Información y Protección de Datos (por su acrónimo, IFAI) es el garante de la protección de los datos personales, tanto en el ámbito privado como en el público. De ahí, que fue esta instancia la encargada idónea para el lanzamiento de dicho documento. Asimismo, participó con aportes importantes en la elaboración del texto, en particular la Dirección General de Clasificación y Datos Personales.

GABRIELA MENDOZA CORREA

Como se ha venido desarrollando, a nivel internacional se han realizado valiosos esfuerzos por establecer reglas para el tratamiento e intercambio de información de las personas al tiempo que se respeta su privacidad. Ese equilibrio se ha podido plasmar en leyes que prevén los principios y derechos de los titulares de los datos, así como el diseño de instituciones que podrían denominarse como ‘órganos garantes’ de la adecuada protección de datos, con independencia y facultades de sanción.³⁷

Más claro, estos órganos coadyuvan a garantizar la salvaguarda del derecho a la privacidad de las niñas, niños y adolescentes, pues de lo contrario se suscitarían implicaciones en su desarrollo y en la consecuente estigmatización social.³⁸

Por lo anterior, puede decirse válidamente que las niñas, niños y adolescentes son sujetos de derechos, entre ellos el de la protección de datos personales, la libre expresión y el derecho al anonimato. La violación de estos derechos en el ámbito de la sociedad de la información y el conocimiento ha traído consigo implicaciones en el desarrollo psicológico, emocional y psicológico de muchos de los niños y adolescentes, ya que en el Internet, estos se enfrentan a situaciones que derivan en riesgos para su seguridad. Como por ejemplo y sin ánimo de exhaustividad, podemos mencionar el *mobbing*, *grooming* o el *cyberbullying*, además de publicidad engañosa, fraudes o actividades ilegales que los pequeños desconocen (juegos de azar, casino *online*, etc.).³⁹

³⁷Para más información sobre la labor de las Agencias de Protección de Datos en el mundo, puede consultarse la página oficial de las Conferencias Internacionales de Autoridades de Protección de Datos y Privacidad, por ejemplo el vínculo relativo a su emisión número 31 que tuvo lugar en Madrid, España: <http://www.privacy-conference2009.org/>

³⁸Milton Friedman, *The Republic of choice. Law, Authority and Culture*, Harvard University Press, Cambridge, 1990, p. 184, citado en José Luis Piñar Mañas, *¿Existe la Privacidad?*, CEU Ediciones, Madrid, 2008, p. 11.

³⁹El nuevo entorno tecnológico ha dado lugar al desarrollo de estos y otros conceptos. En concreto, la ciber –intimidación ha sido definida como “la promoción del comportamiento hostil o humillante de algún individuo que tiene la intención de hacer daño a otros individuos por medio del uso de la tecnología informática y comunicaciones como por ejemplo, el correo electrónico, teléfonos celulares, mensajes textuales, mensajes instantáneos y sitios de web personales. El acoso virtual, por otra parte, refiere al mismo tipo de comportamientos pero con la particularidad de que estos se realizan a través de la red social de la persona o la organización a quien se calumnia o descalifica. Específicamente, a través de tecnologías de carácter

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Al respecto, cabe mencionar brevemente el peligro que supone para las niñas, niños y adolescentes el uso de pseudónimos, o bien, de identidades anónimas por parte de pedófilos. Internet tiene un significado especial para los pedófilos ya que les proporciona un foro que:

- Permite intercambios personales íntimos;
- Permite llevar a cabo estos intercambios bajo condiciones relativamente seguras (anonimato), y
- Posibilita intercambios que no están restringidos por barreras geográficas o costos.

Esta última característica es importante, pues entre más pequeño sea el tamaño del colectivo en un contexto dado, más aislado se sentirá. De esta forma, la red neutraliza la barrera de la distancia y aumenta la probabilidad de alcanzar una masa crítica para el desarrollo de una minoría importante.⁴⁰

Pueden darse, además, abusos de datos personales que pueden derivar en la vulneración de derechos de privacidad, de la propia imagen e intimidad de las niñas, niños y adolescentes. El anonimato, aunado a la ausencia de supervisión, hace que en muchas ocasiones los derechos de la infancia y la adolescencia puedan verse vulnerados. En consecuencia, se hace necesario revisar cuáles son estos derechos y garantizar de manera efectiva las medidas legislativas y educativas que contribuyan a su cumplimiento.

A este respecto, en 2004 la UNICEF promulgó un decálogo básico de cuáles deberían ser los derechos de las niñas, niños y adolescentes en Internet, basado en el documento titulado “Los e-derechos de los niños y niñas”.

colectivo, tales como sitios web, foros, *blogs* y listas de correos”. Véase el estudio de María Frick, *Niños y jóvenes en la Sociedad de la Información. Acceso y uso de Internet en América Latina*, Centro Euro-Latinoamericano (CEULA), Instituto de Empresa (IE), Telefónica, Madrid, octubre, 2007, p. 14.

⁴⁰Véase Elena Azaola y Richard J. Estes (coord.), *La infancia como mercancía sexual. México, Canadá, Estados Unidos*, Siglo Veintiuno Editores en coedición con el Centro de Investigaciones y Estudios Superiores en Antropología Social, México, 2003, p. 124.

GABRIELA MENDOZA CORREA

DECALOGO DE DERECHOS DE LAS NIÑAS, NIÑOS Y ADOLESCENTES EN LAS TIC⁴¹

1. Derecho al acceso a la información y la tecnología sin discriminación por sexo, edad, recursos económicos, nacionalidad, etnia y lugar de residencia. Especialmente si son discapacitados.
 2. Derecho a la libre expresión y asociación. A buscar, recibir y difundir informaciones e ideas en la red. Este derecho solo podrá ser restringido en el caso de que se ponga en riesgo el bienestar, desarrollo e integridad de los niños y niñas.
 3. Derecho a que sean consultados y a dar su opinión cuando les afecte.
 4. Derecho a la protección contra la explotación, el comercio ilegal, los abusos o la violencia que use Internet como medio. Tendrá derecho a utilizar Internet para conocer y defender sus derechos.
 5. Derecho al desarrollo personal y a la educación que Internet pueda aportarles para su formación.
 6. *Derecho a la intimidad de sus comunicaciones por medios electrónicos. Derecho a preservar su identidad e imagen de usos ilícitos.*
 7. Derecho al ocio, la diversión y el juego mediante las TIC y a que éstos no contengan violencia gratuita, mensajes racistas, sexistas o denigrantes y respeten los derechos a la propia imagen.
 8. Los padres y madres tienen el derecho y la responsabilidad de orientar, educar y pactar con sus hijos e hijas el uso responsable de Internet.
 9. Los gobiernos deben comprometerse a cooperar con otros países para facilitar el acceso a Internet de los niños y niñas.
 10. Derecho a utilizar en su favor las TIC siendo respetuosos con el medio ambiente y los derechos de los demás.
-

⁴¹Disponible en su totalidad en el vínculo electrónico siguiente: <http://www.ciberderechos-infancia.net/e-derechos-unicef.html> [Énfasis añadido].

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

Dado el escenario actual, es urgente que los Estados expidan normatividad en la materia de protección de datos, libertad de expresión, el derecho al anonimato y al uso de pseudónimos para los niños y adolescentes, además de la homologación transfronteriza de dichas normas. Asimismo, que las autoridades en todos sus niveles, se enfoque en la prevención a través de la educación.

El uso de las redes sociales, y en general de la sociedad de la información y el conocimiento —por su carácter transversal— requiere de la cooperación internacional y de una aproximación a la ciber-seguridad de forma integral, desde perspectivas jurídicas, técnicas, humanistas, económicas, procedimentales y multi-agencias, entre otros.

Aunado a ello, la protección a la infancia en el ámbito tecnológico urge del apoyo parental y tutorial, de el ámbito educativo, de normatividad eficaz y políticas de seguridad de proveedores de Internet eficientes, en virtud de que la protección al menor requiere del esfuerzo conjunto.

De ahí que la socialización del *Memorándum de Montevideo*, contribuye a la transformación cultural a partir de la construcción de una ciudadanía digital responsable, desde la infancia.

Internet refleja la compleja sociedad en la que vivimos. Para los niños las nuevas tecnologías son una oportunidad para acceder a nuevas formas de aprendizaje, de divertirse y de comunicarse. Pero también, existe un mundo de adultos donde la pornografía, la violencia y las actividades delictivas tienen su referencia virtual. Los padres y educadores tienen el deber de orientar a los niños para que sus experiencias en estos medios sean positivas y seguras.

La responsabilidad, han coincidido los expertos que elaboraron el *Memorándum de Montevideo*, radica en varios actores y requiere de una perspectiva amplia de aproximación, así como fomentar la creación de capacidad y la cooperación internacional. Si bien, en la tarea educadora, el ámbito familiar es el primer implicado, sin embargo debe realizarse en sintonía y con una apuesta sistematizada y curricular en el contexto escolar, con el apoyo de la sociedad en general, de desarrolladores, medios de comunicación, procuradores de justicia, y autoridades y entidades educativas.

GABRIELA MENDOZA CORREA

La incorporación al uso de Internet es cada vez a edades más tempranas y por ello, hay que intervenir desde las primeras etapas, al ser los niños de estas generaciones nativos digitales. De tal forma que es necesario apoyar a las nuevas generaciones para su desarrollo como ciudadanos en el nuevo contexto digital, esto es, de un navegante seguro se ha de evolucionar a un ciudadano digital. La ciudadanía digital se apoya en cuatro pilares básicos: alfabetización digital, la alfabetización en los medios audiovisuales, la alfabetización social y la alfabetización cultural. La prioridad es la prevención basada en la educación, sin dejar de lado un enfoque multidisciplinario. A través de la educación y la participación activa de los niños y adolescentes, así como con ayuda de los docentes y padres de familia, en esfuerzo conjunto y tomando en consideración el principio fundamental del interés superior de niñas, niños y adolescentes. Solo de esta forma, se podrá contribuir a la formación de ciudadanos digitales responsables.

Un estudio publicado por la Unión Internacional de Telecomunicaciones,⁴² titulado “Protección de la Infancia en Línea” arroja que a finales de 2008, había más de 1.500 millones de personas en línea en comparación con menos de 200 millones a comienzos de 1998. El mismo reporte indica que alrededor del 90 por ciento de adolescentes y jóvenes adultos utilizan el Internet; más del 60 por ciento de niños y adolescentes conversan cotidianamente en sitios de charla; tres niños de cada cuatro están dispuestos a compartir en línea información personal sobre ellos mismos y su familia, a cambio de bienes y servicios; un niño de cada cinco será contactado por un predador o pedófilo cada año; aunque el 30 por ciento de los adolescentes mencionan el acoso sexual padecido en una sala de charla, solo el 7 por ciento lo cuenta a sus padres, por miedo a que pongan límites a su acceso en línea.

En México, por citar un ejemplo próximo, las estadísticas del Gobierno Federal,⁴³ señalan que la explotación sexual de niñas, niños y adolescentes a través de Internet ocupa el tercer lugar en la

⁴²Disponible en el vínculo: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>

⁴³Véase, *Informe Global de Monitoreo de las acciones en contra de la explotación sexual comercial de niños, niñas y adolescentes*, Sección México, p. 13. Disponible en el vínculo: <http://www.derechosinfancia.org.mx/Global%20Monitoring%20Report-MEXICO.pdf>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

lista de delitos cibernéticos, sólo antecedida por los fraudes y amenazas. Además, afirma que los sitios en la red incrementan a ritmos acelerados. Mientras que en enero de 2004 se registraron 72 mil 100 sitios de pornografía sexual de niñas, niños y adolescentes, a inicios del 2006 ya existían más de 100 mil sitios. Además, México es considerado el segundo país a nivel mundial con mayor producción de pornografía infantil.⁴⁴

La solución no es dar la espalda al Internet, porque su uso es algo necesario en nuestra realidad. Lo importante es dotar de estrategias y recursos al menor para que pueda enfrentarse a la red, mediante un adecuado asesoramiento pedagógico y una colaboración positiva entre familia y escuela, que se presentan como variables importantes en la vida de los niños y jóvenes.

El control desde el propio individuo se caracteriza porque son los padres y profesores los que ayudan a tomar las decisiones correctas sobre Internet. Se debe educar a que actúen y tomen decisiones informadas, tomando en consideración su derecho al anonimato, y el balance con el derecho a la libre expresión.

Reflexiones a manera de conclusión. El balance entre la protección y la libertad de expresión en línea

Si bien, este texto expone intrínsecamente dos posiciones aparentemente contradictorias ante el uso del entorno tecnológico por parte de los niños y adolescentes, cabe precisar que estas posturas no necesariamente se contraponen. Un documento recientemente publicado clarifica el objeto de este texto de forma más clara, me refiero al documento conclusivo del “Foro de Discusión del Instituto de Internet de Oxford sobre la Protección de la Infancia y la Libertad de Expresión en Línea (2010)”.⁴⁵ En él se hace explícito que los

⁴⁴Senado de la República, “Del Senador Adolfo Toledo Infanzón, del Grupo Parlamentario del PRI, la que contiene punto de acuerdo de la pornografía infantil vía Internet”, *Gaceta Parlamentaria*, Número 21, Año 2006. Disponible en el vínculo: <http://www.senado.gob.mx/sssp/gaceta/?sesion=2006/11/16/1&documento=30> Además, Secretaría de Seguridad Pública, *Estadística Pedofilia en Internet*. Disponible en el vínculo: http://www.ssp.gob.mx/application?pageid=home_sub_2&docId=2794 y citado en *Informe Global de Monitoreo... Op. cit.*

⁴⁵Los defensores de ambos lados del debate se reunieron en octubre de 2009 para

GABRIELA MENDOZA CORREA

defensores de la protección de los niños y la libertad de expresión en línea comparten la convicción de proteger los derechos humanos básicos.

No obstante dicha convicción, ha disminuido el número de políticas alternativas disponibles para enfrentar las amenazas tanto a la seguridad de la niñez como a la libertad de expresión en línea, dando como resultado que frecuentemente se presenten dichos intereses como si fuesen diametralmente opuestos.

Los participantes lograron identificar el terreno común, mediante la definición de un nuevo marco para discutir la protección de la infancia en línea que rechace el pánico moral presente que domina la discusión, y antes bien, se concentre en la definición precisa de los riesgos en conjunción con la evolución de las capacidades de las niñas, niños y adolescentes.

Las opciones más fructíferas han sido planteadas por la necesidad de precisión y transparencia en las políticas para abordar estos temas. Gracias a la colaboración de estas dos visiones, se puede continuar con la protección de la infancia al tiempo que se impide que esta se use como pretexto estratégico para alcanzar objetivos más amplios de la censura y la represión.

Podemos también concluir que el anonimato o la no-identificación funcional es un fenómeno que yace en la intersección entre la ley, la política y la tecnología con implicaciones para el comercio, la libertad individual, para nuestra forma de vida y la interacción social. Combinar el trabajo legal y político con las herramientas técnicas para mantener la capacidad de Internet de servir como vehículo de la libre expresión, es imperativo.

Los proveedores de acceso a Internet son responsables de informar al público sobre los riesgos que conlleva el uso de sus redes. Deberán reportar las tecnologías que representen peligros a la privacidad y ofrecer acceso a aplicaciones que respeten la intimidad. Los proveedores del servicio tienen un papel importante al actuar como guardianes entre los usuarios y la red.

explorar sus diversas perspectivas respecto a los derechos fundamentales y para identificar las áreas de acuerdo. A. Powell, M. Hills y V. Nash, *Child Protection and Freedom of Expression Online*, Oxford Internet Institute Discussion Forum Paper No. 17, Oxford, 2010. Para consultar el reporte en su totalidad véase el vínculo siguiente: <http://www.oii.ox.ac.uk/news/?id=405>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

De forma paralela, es necesario proveer a la sociedad de herramientas para controlar los desarrollos tecnológicos que podrían amenazar la sobrevivencia de las libertades individuales y colectivas. De ahí que lo importante no es la tecnología en sí misma, sino nuestra capacidad como ciudadanos para afirmar nuestro derecho a la libre expresión y a la privacidad de la comunicación.

En definitiva, el anonimato es una herramienta más que ya está aquí, para la que hay motivos de uso. Los daños que pueda provocar, al igual que los daños que pueda provocar cualquiera de las herramientas comentadas en este informe, no podrán evitarse con la prohibición, y tampoco evitarán estos usos ilícitos. De ahí que la posición sensata es la de precaución y prevención a través de la educación y el involucramiento de todas las variables sociales que están inmersas en la vida cotidiana de los menores, al tiempo que se les educa y empodera. Sólo de esta forma alcanzaremos el balance entre el entusiasmo y el miedo en el sentido del uso responsable de las nuevas tecnologías.

Referencias bibliográficas

- AZAOLA Elena y Richard J. ESTES (coord.) (2003), *La infancia como mercancía sexual. México, Canadá, Estados Unidos*, Siglo Veintiuno Editores en coedición con el Centro de Investigaciones y Estudios Superiores en Antropología Social, México.
- FRICK María (2007), *Niños y jóvenes en la Sociedad de la Información. Acceso y uso de Internet en América Latina*, Centro Euro-Latinoamericano (CEULA), Instituto de Empresa (IE), Telefónica, Madrid.
- FRIEDMAN, Milton (2008), *The Republic of choice. Law, Authority and Culture*, Harvard University Press, Cambridge.
- FROOMKIN, Michael (2003), "Anonymity in the Balance", en C. Nicoll, J.E. Prins y M.J. van Dellen (eds.), *Digital Anonymity: Tensions and Dimensions*, Cambridge University Press, Cambridge. Disponible el formato digital en el vínculo: <http://osaka.law.miami.edu/~froomkin/articles/balance.pdf>

GABRIELA MENDOZA CORREA

- (2000), “The Dead of Privacy”, *Stanford Law Review*, Vol. 52, Stanford University, pp. 1461-1563. Disponible el formato digital en el vínculo: <http://osaka.law.miami.edu/~froomkin/articles/privacy-deadthof.pdf>
- (1995), “Anonymity and Its Enmities”, *Journal of Online Law*, University of Miami. Disponible el formato digital en el vínculo: http://articles.umlaw.net/froomkin/Anonymity_Enmities.htm
- GARCÍA CANCLINI, N. (2004), *Diferentes, desiguales y desconectados. Mapas de la Interculturalidad*, Gedisa Editorial, Barcelona.
- GRIJPINK J. y C. PRINS (2001), “New Rules for Anonymous Electronic Transactions?. An Exploration of the Private Law Implications of Digital Anonymity”, *Computer Law & Security Report*, The University of Warwick, Vol. 17, No. 6, pp. 379-389.
- MURILLO DE LA CUEVA, Pablo y José Luis Piñar Mañas (2009), *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid.
- PIÑAR MAÑAS, José Luis (2009), *¿Existe la Privacidad?*, CEU Ediciones, Madrid.
- POULLET Y. (2007), “Hacia nuevos principios de protección de datos en un nuevo entorno TIC”, *Revista d'Internet, Dret i Política*, Universitat Oberta de Catalunya, No. 5, España.

Ligas consultadas

- Convención sobre los derechos del niño adoptada el 20 de noviembre de 1989 y disponible en el vínculo siguiente: <http://www2.ohchr.org/spanish/law/crc.htm>
- La Convención No. 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal está disponible en el vínculo electrónico siguiente: <http://conventions.coe.int/treaty/en/treaties/html/108.htm>
- La Decisión del Consejo de la Unión Europea del 29 de mayo

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

de 2000, relativa a la lucha contra la pornografía infantil en Internet, puede consultarse en el vínculo electrónico siguiente: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0375:ES:HTML>

Libro Verde sobre la Protección de Menores y de la Dignidad en los Servicios Audiovisuales y de Información. Disponible para su consulta en el vínculo electrónico siguiente: http://europa.eu/legislation_summaries/audiovisual_and_media/l24030_es.htm

Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Disponible en el vínculo siguiente: http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/ESP_CONV.pdf

Opinión 5/2009 sobre redes sociales en línea del Grupo de Trabajo de Protección de Datos de la Comisión Europea. Disponible en el vínculo siguiente: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Memorándum de Montevideo. Disponible en la versión en español en el vínculo siguiente: <http://memorandumdemontevideo.ifai.org.mx/>

Zero Knowledge Systems sobre encriptación y anonimato, fundada en 1997 y disponible en el vínculo electrónico siguiente: <http://www.zeroknowledge.com/>

Internet, libertad y sociedad: una perspectiva analítica del curso académico 2001-2001 de la *Universitat Oberta de Catalunya* y pronunciado por el profesor Manuel Castells, catedrático del Instituto Interdisciplinario de Internet de la misma universidad. Disponible en el vínculo siguiente: http://www.uoc.edu/web/esp/launiversidad/inaugural01/intro_conc.html

Reporte sobre la aplicación de los principios de protección de datos en la Red Mundial de Telecomunicaciones. Disponible en el vínculo electrónico siguiente: http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD%20documents/T-PD%20_2004_%2004%20E%20final%20Report%20POULLET.pdf

GABRIELA MENDOZA CORREA

“Protección de la Infancia en Línea” de la Unión Internacional de Telecomunicaciones. Disponible en el vínculo: <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>

Recomendación 3/97 de 3 de diciembre de 1997 sobre el anonimato en Internet. Disponible para su consulta en el vínculo electrónico siguiente: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp6_es.pdf

Memorándum de Budapest-Berlín sobre protección de datos e intimidad en Internet. Disponible en el vínculo electrónico siguiente: <http://www.informatica-juridica.com/anexos/anexo508.asp>

Recomendación No. R (99) 5 del Comité de Ministros del Consejo de Europa, disponible en el vínculo siguiente: <http://www.informatica-juridica.com/anexos/anexo197.asp>

Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, disponible en el vínculo siguiente: http://europa.eu/legislation_summaries/information_society/l14012_es.htm

Directiva 2002/58/CE del Parlamento Europeo y del Consejo del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponibles en el vínculo electrónico siguiente: http://europa.eu/legislation_summaries/information_society/l24120_es.htm

Estándares Internacionales sobre Protección de Datos Personales y Privacidad (“Estándares de Madrid”). Disponible en el vínculo electrónico siguiente: https://www.agpd.es/portal-webAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

Reporte sobre la aplicación de los principios de protección de datos en la Red Mundial de Telecomunicaciones. Disponible en el vínculo electrónico siguiente: <http://www.coe.int/t/>

PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES

dghl/standardsetting/dataprotection/TPD%20documents/
 T-PD%20_2004_%2004%20E%20final%20Report%20
 POULLET.pdf

Resolución sobre Protección de la Privacidad en los servicios de re-
 des sociales. Disponible en el vínculo electrónico siguiente:
https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/30_conferencia_internacional/resolucion_redes_sociales.pdf

McIntyre v. Ohio (1995). Disponible en el vínculo siguiente: <http://www.law.cornell.edu/supct/html/93-986.ZO.html>

Ley Federal de Protección de Datos Personales en Posesión de los
 Particulares de México. Disponible para su consulta en el
 vínculo electrónico siguiente: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

Informe Global de Monitoreo de las acciones en contra de la ex-
 plotación sexual comercial de niños, niñas y adolescentes,
 Sección México. Disponible en el vínculo: <http://www.derechosinfancia.org.mx/Global%20Monitoring%20Report-MEXICO.pdf>

Senado de la República, “Del Senador Adolfo Toledo Infanzón,
 del Grupo Parlamentario del PRI, la que contiene punto de
 acuerdo de la pornografía infantil vía Internet”, Gaceta Parla-
 mentaria, Número 21, Año 2006. Disponible en el vínculo:
<http://www.senado.gob.mx/sgsp/gaceta/?sesion=2006/11/16/1&documento=30>

Secretaría de Seguridad Pública, *Estadística Pedofilia en Inter-
 net*. Disponible en el vínculo: http://www.ssp.gob.mx/application?pageid=home_sub_2&docId=2794

Decálogo UNICEF: Los e-derechos de los niños y las niñas (2004).
 Disponible en el vínculo: <http://www.ciberderechos-infancia.net/e-derechos-unicef.html>

Documento del Foro de Discusión del Instituto de Internet de Ox-
 ford sobre la Protección de la Infancia y la Libertad de Ex-
 presión en Línea (2010). Disponible en formato digital en el
 vínculo: <http://www.oii.ox.ac.uk/news/?id=405>