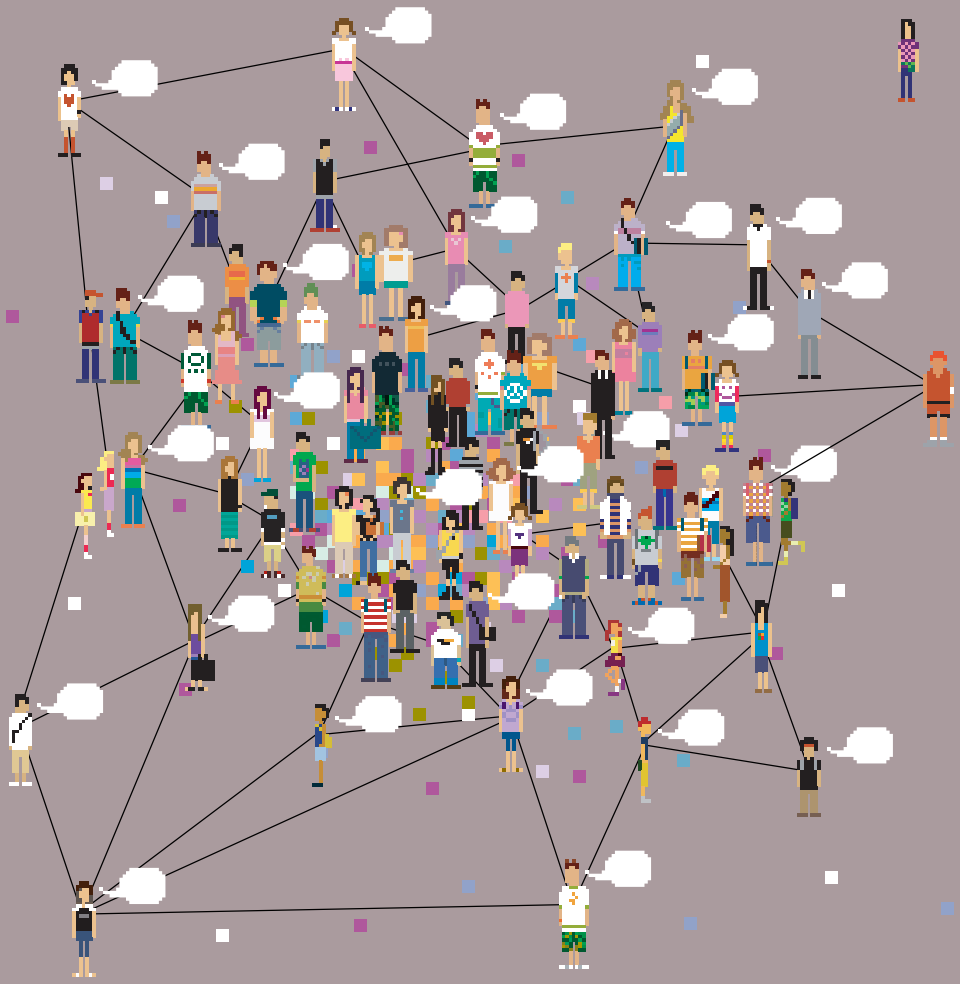


PROTECCIÓN DE DATOS PERSONALES EN LAS REDES SOCIALES DIGITALES: EN PARTICULAR DE NIÑOS Y ADOLESCENTES.

MEMORÁNDUM DE MONTEVIDEO

Carlos G. Gregorio – Lina Ornelas
Compiladores

Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes

Memorándum de Montevideo

La investigación presentada en esta publicación es fruto de un proyecto apoyado por el Centro de Investigaciones para el Desarrollo (www.idrc.ca) y de la Agencia Canadiense de Desarrollo Internacional (www.acdi-cida.gc.ca), Ottawa, Canadá. Las opiniones expresadas en esta publicación son propias de los autores y no necesariamente representan las del IDRC o su Junta de Gobernadores o las de la ACDI.

IDRC CRDI

Canadian International Development Agency | Agence canadienne de développement international

Carlos G. Gregorio – Lina Ornelas

Compiladores

Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes

Memorándum de Montevideo

IIJusticia

Instituto de Investigación para la Justicia

ifai

Instituto Federal de Acceso a la Información y Protección de Datos

Instituto Federal de Acceso a la Información y Protección de Datos

Av. México, 151

México, D.F., México

Integrantes del Pleno

Jacqueline Peschard Mariscal

Comisionada Presidenta

Sigrid Arzt Colunga

Comisionada

María Marván Laborde

Comisionada

María Elena Pérez-Jaén Zermeño

Comisionada

Ángel Trinidad Zaldívar

Comisionado

Alejandro Del Conde Ugarte

Secretario de Protección de Datos Personales

Cecilia Azuara Arai

Secretaria de Acuerdos

Mauricio Farah Gebara

Secretario Ejecutivo

Instituto de Investigación para la Justicia

Lavalle 1125

Buenos Aires, Argentina

Carlos G. Gregorio

Presidente

Gladys S. Álvarez

Vicepresidente

Norma O. Silvestre

Secretaria

Primera edición: julio 2011

Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo / compilado por Carlos G. Gregorio y Lina Ornelas
1ª ed., México, 2011
288 p.; 14 x 21.5 cm.
ISBN – 13: 978-968-5954-59-4

1. Derechos Humanos, 2. Protección de datos personales.
I. Gregorio, Carlos G., comp. II. Ornelas, Lina comp.

DIRECCIÓN EDITORIAL
Dra. Gabriela Mendoza Correa

Impreso y hecho en México

Índice

Presentación

El *Memorándum de Montevideo*: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana

Chantal Bernier[*]

El *Memorándum de Montevideo* vio la luz después de la elaboración del Informe de Investigación de la Comisionada de Protección de Datos Personales de Canadá sobre *Facebook* (julio de 2009), aunque está basado en un análisis social y jurídico independiente, decididamente iberoamericano, orientado por el Grupo multidisciplinario y multinacional de expertos de Montevideo.

Este fondo empírico y jurídico guió la elaboración de ese documento de referencia, asegurando de ese modo su pertinencia respecto a los desafíos de la era digital y teniendo en cuenta la realidad social y jurídica de la región iberoamericana. La experiencia de nuestra Comisionada en la investigación relativa a *Facebook* contribuyó a la elaboración del *Memorándum de Montevideo* para reflejar en dicho documento los desafíos y soluciones jurídicas y económicas fruto de la encuesta, la cual dio lugar a la modificación de los parámetros de confidencialidad de *Facebook* en todo el mundo.

[*]La autora es Licenciada en Derecho Civil por la Universidad de Sherbrooke y cuenta con una maestría en Derecho Público Internacional por la Universidad de Londres. Actualmente ocupa el cargo de Comisionada Adjunta de Protección de los Datos Personales de Canadá en la Oficina de Privacidad.

La Comisionada de Protección de Datos Personales de Canadá participó en la elaboración del *Memorándum de Montevideo* guardando una distancia respetuosa y, al mismo tiempo, comprometiéndose profundamente. La distancia venía dictada por el hecho de que Canadá no forma parte de la región iberoamericana. Nuestro compromiso emanaba del reconocimiento a las dimensiones internacionales de la protección de los datos personales en la era digital, la importancia de los desafíos a la protección de los datos personales de los más jóvenes en Internet y la urgencia de elaborar marcos normativos que puedan orientar a los Estados y las empresas en sus esfuerzos para responder a esos desafíos.

La importancia del *Memorándum de Montevideo* se puede resumir en cuatro puntos que abordaré individualmente, a saber; su sólida base empírica, su marco normativo claro, pertinente y exhaustivo, su estructura dirigida específicamente a los distintos actores en juego y su rigor jurídico.

1. La base empírica del *Memorándum de Montevideo*

El *Memorándum de Montevideo* es fruto de investigaciones sociales y jurídicas exhaustivas. El punto de partida para la creación de este documento de referencia procede de una investigación aplicada que contó con el apoyo –entre otros–, de encuentros con grupos de jóvenes en los que se examinaron sus costumbres, usos, actitudes y experiencias acerca de Internet, así como sus expectativas con respecto a la protección de sus datos personales. Así pues, la elaboración de este documento de referencia sobre las políticas, medidas y normas que deben regir la protección de los jóvenes en Internet se benefició de datos empíricos sólidos y exhaustivos para identificar los desafíos reales que deben superarse. Como resultado de ello, las disposiciones del Memorándum proponen medidas que responden de forma adecuada al contexto real de las actividades y a los riesgos en las redes sociales para los jóvenes en la región iberoamericana.

Este enfoque consistió en definir de forma rigurosa el fenómeno social y el contexto jurídico antes de elaborar el correspondiente marco normativo, como el primero de los elementos valiosos del *Memorándum de Montevideo*. En este sentido, constituye la garantía de su pertinencia.

2. Un marco normativo claro, pertinente y exhaustivo

A partir del análisis empírico de los riesgos, aunque también de las oportunidades del fenómeno social en Internet en la región iberoamericana, se elaboró un marco normativo. El objetivo era conciliar por una parte, la realidad de los riesgos y las intrusiones en la vida privada de los jóvenes en Internet en la región iberoamericana y, por otra, el estado de derecho aplicable.

Por consiguiente, el *Memorándum de Montevideo* fue concebido a medida, por decirlo de alguna manera, para responder a la realidad social, cultural y jurídica de la región iberoamericana. Cada medida normativa o legislativa propuesta se fundamenta en la tradición jurídica iberoamericana, sus valores subyacentes y la realidad de sus movimientos sociales y culturales. El resultado es un documento que responde a los imperativos sociales y jurídicos de la región, y ofrece un marco normativo fundamentado en principios de derecho y en su sistema jurídico. Por lo tanto, el marco normativo propuesto por el Memorándum se puede implementar de forma coherente con el contexto jurídico existente. Ésta es su segunda gran ventaja; una armonización al mismo tiempo flexible, y vinculada con el contexto político, social y jurídico iberoamericano.

3. Una estructura centrada de forma eficaz en los principales actores

Habida cuenta de que procede de un análisis de los desafíos reales de la protección de datos personales de los jóvenes en Internet, el *Memorándum de Montevideo* ha identificado naturalmente a los principales actores responsables de dicha protección. Así pues, el Memorándum está estructurado en torno a las responsabilidades de esos actores, a saber; las autoridades educativas, las autoridades de políticas públicas, las autoridades legislativas y las empresas de la industria Internet. La responsabilidad de los actores se define en referencia al artículo 16 de la *Convención sobre los derechos del niño*, que estipula lo siguiente:

> 16. …
>
> 1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
>
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.

La elección de este enfoque, es decir, anclar el Memorándum en la *Convención sobre los derechos del niño* y, más concretamente, en la obligación estipulada en el apartado (2) del artículo 16 de promulgar leyes para proteger al niño contra cualquier ataque a su vida privada, consolida la fuerza normativa del Memorándum. Aun cuando las disposiciones del documento no sean vinculantes, este apuntalamiento en los cimientos inquebrantables de la *Convención sobre los derechos del niño* le asegura una importante influencia.

A partir de esta premisa, la división del marco normativo entre los principales actores –precisando sus respectivas responsabilidades–, facilita la aplicación del Memorándum: el reparto de las responsabilidades está claramente delimitado, las expectativas se definieron adecuadamente y se perfilaron una serie de medidas concretas, prácticas y realistas para proteger la vida privada de los jóvenes en Internet.

Esta estructura hace que el Memorándum sea una auténtica herramienta de trabajo que apoya al mismo tiempo los procesos de toma de decisiones en cuestión y la implementación de las medidas correspondientes.

4. El rigor jurídico

Paralelamente, el *Memorándum de Montevideo* destaca por su fidelidad a los regímenes jurídicos de la región iberoamericana. Cada una de sus disposiciones ha sido debatida a fin de asegurar su coherencia con las leyes existentes y los principios de derecho aplicables, así como su compatibilidad con los regímenes constitucionales establecidos. Las cuestiones centrales de la competencia territorial, la responsabilidad civil y contractual o los recursos judiciales se abordan de forma innovadora y pragmática.

Este análisis trata de subsanar el distanciamiento jurídico que persiste entre, por una parte, el marco legal que rige Internet en la región iberoamericana y, por otra, el desarrollo tecnológico de nuevas aplicaciones, contenidos y usos de Internet relacionados con las tendencias sociales, las prácticas comerciales o una nueva forma de criminalidad.

Así, los elaboradores de políticas públicas y los gerentes de empresas de servicios de Internet encontrarán en el *Memorándum de Montevideo* un marco de referencia único y esencial para sus procesos de toma de decisiones, ya sea con relación a la elaboración de medidas sociales, políticas, legislativas o comerciales, o respecto al desarrollo de nuevas aplicaciones tecnológicas. Las disposiciones del documento constituyen una guía para la integración de la protección de los datos personales de los jóvenes en Internet.

Ante el impresionante auge de las actividades de los jóvenes en Internet, documentadas por estadísticas que revelan que más del 90% de los jóvenes de entre 12 y 17 años están en línea, y ante la incidencia creciente de intrusiones, ya sea con fines comerciales o criminales, las medidas propuestas por el *Memorándum de Montevideo* se imponen como una necesidad urgente.

La Comisionada de Protección de Datos Personales de Canadá reconoce con profunda admiración el trabajo del Grupo de expertos de Montevideo y considera el Memorándum un auténtico documento de referencia sobre la protección de datos personales de los jóvenes en Internet. Por ello seguimos con gran esperanza su difusión entre los Estados y empresas de la región iberoamericana, como un modelo para el mundo entero.

Chantal Bernier

Comisionada Adjunta de Protección de los Datos Personales de Canadá

Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos

Jacqueline Peschard Mariscal[*]

Es un lugar común afirmar que hoy en día vivimos la era digital, en donde gracias al avance de las tecnologías de la información el Internet se ha convertido en un medio de comunicación plenamente socorrido, al punto que forma parte ya del desarrollo de nuestras actividades cotidianas. Son muchas las ventajas que el Internet ofrece, pues sin lugar a duda, es un recurso educativo que permite incrementar nuestros conocimientos y acceder rápidamente a información que hace apenas unos lustros resultaba prácticamente inimaginable.

Asimismo las redes sociales en Internet han devenido herramientas de comunicación multifuncionales, que nos permiten entrar en contacto con personas de todo el mundo y compartir experiencias de muy variado tipo en esta nueva aldea global. Es así como, las redes sociales permiten obtener, almacenar y transmitir un sin número de datos, documentos, fotografías, videos, música –entre otros–, y el acceso a éstos es tan sencillo con simplemente un clic.

[*]La autora es Doctora en Ciencias Sociales por El Colegio de Michoacán. Es miembro del Sistema Nacional de Investigadores y de la Academia Mexicana de Ciencias. Desde abril del 2009 ocupa el cargo de Comisionada Presidenta del Instituto Federal de Acceso a la Información y Protección de Datos en México.

La sociedad de la información y la comunicación necesariamente debe tener como su centro de atención a las personas; esto es, la aproximación a la sociedad de la información y la comunicación desde una perspectiva basada en 'derechos' implica colocar la dignidad humana, el desarrollo humano y los derechos como ciudadanos globales y digitales por encima de las consideraciones tecnológicas o la relación comercial productor-consumidor. Más aun, implica educar en la ciberciudadanía y proteger en este ámbito a las niñas, niños y adolescentes para garantizar una navegación segura.

Sin lugar a duda, las redes sociales han significado una revolución en la forma de comunicarnos, y son los jóvenes, los adolescentes y también las niñas y los niños los usuarios más frecuentes, porque encuentran en ellas oportunidades de conocimiento, de entretenimiento, de diversión y también de socialización, ya que con frecuencia para formar parte de estas redes hay que registrar un perfil del usuario al que después se invita a pertenecer a amigos y conocidos, formándose así un complejo tejido de relaciones sociales, que si bien ofrece una atractiva interacción, los expone a una serie de riesgos.

Esta exposición constante y pública de la información en las redes sociales que implica ciertos peligros, es particularmente importante cuando es relativa a los menores de edad porque pueden acceder a contenidos de información que no son pertinentes para su edad o entrar en contacto con personas que explotan su información; esa información que circula con gran fluidez pudiendo ser objeto de discriminación, de difamación, de violencia psicológica e incluso de acoso sexual o pornografía. Todos estos riesgos pueden dañar el desarrollo integral del niño y del adolescente.

La experiencia reciente muestra que en todos los países han ocurrido afectaciones al desarrollo de la personalidad de los menores de edad, derivadas de las invasiones a espacios de intercambio de información e imágenes que los niños y adolescentes frecuentan. Frente a la vulnerabilidad de los menores de edad en estas nuevas formas de convivencia social a través de las redes sociales en Internet, el derecho no puede quedarse rezagado.

Internet es un espacio lleno de oportunidades, especialmente para los jóvenes, y en consecuencia, debe existir un balance entre el despliegue de la libertad de expresión y la protección de su dignidad

como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información con otros en los ambientes digitales. Sin embargo, habrá que hacer conciencia que el ciberespacio no es un espacio virtual, sino que forma parte de nuestro un espacio 'real'.

El Internet es un espacio que nos brinda grandes libertades, y por esa razón exige grandes responsabilidades del adulto que está cerca del menor, y de los propios niños, niñas y adolescentes.

Si bien es cierto, el avance tecnológico y la vinculación de los menores con las nuevas tecnologías representa un elemento del proceso evolutivo de la sociedad, también es cierto que este nuevo espacio debe ser regulado para proteger los derechos de la niñez en todos sus ámbitos. Es así como la protección de los datos personales y de la integridad del niño, demandan de un esfuerzo conjunto y de una aproximación holística –atendiendo a la diversidad social, cultural, política y normativa–. Los menores de hoy son nativos digitales y su atención involucra necesariamente un enfoque integral e interdisciplinario, más aun nos demanda la aplicación de una visión preventiva a través de la educación y la concientización con afán preventivo.

En este sentido, el papel del Estado es garantizar la convivencia y el balance adecuado entre ambos derechos, es decir, de la libertad de expresión y de la protección a los derechos de la privacidad, estableciendo con claridad que el Internet no es un espacio sin ley. En consecuencia, el propósito de las autoridades de protección de datos y otras instituciones deberá ser el de garantizar una navegación segura a través de un conjunto de normas y políticas públicas que fomenten el pleno conocimiento de las consecuencias que conlleva la participación en redes sociales.

Se pretende que el Estado logre que la industria de las redes sociales se responsabilice de que el servicio que ofrece alerte y proteja a los usuarios frente a invasiones indebidas o ilegales a su vida privada.

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" referido también como *Memorándum de Montevideo*, contiene una serie de recomendaciones dirigidas a organismos gubernamentales, a legisladores, a jueces, pero también a la sociedad y a la industria de las redes sociales para que en el ám-

bito de sus respectivas competencias, se comprometan a trabajar a favor de la protección de los menores y de sus datos.

El Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) en su carácter de autoridad garante de la protección de datos personales en la Administración Pública Federal mexicana como en el ámbito privado, ha querido sumarse al esfuerzo del Centro Internacional de Investigaciones para el Desarrollo (IDRC), para extender los aspectos positivos de la información y el conocimiento, incluyendo desde luego, al Internet y a las redes sociales, a la vez que para prevenir aquellas prácticas perjudiciales o impactos negativos que conllevan y que suelen ser difíciles de revertir una vez que han hecho daño.

Conscientes de que la sociabilización en la región de este documento, implica comprender que el Internet no tiene fronteras y, en este sentido que se requiere de un esfuerzo conjunto sin límites, el 3 de diciembre de 2009 se presentó el *Memorándum de Montevideo* en la Ciudad de México, congregando a los representantes de la industria, medios de comunicación, legisladores, jueces, padres de familia, organizaciones de la sociedad civil y autoridades en educación con el objeto de fomentar el diálogo, conocer el estado que guarda la cuestión en nuestra región, definir las estrategias y alentar a la adopción de políticas públicas encaminadas a la protección de los menores en Internet.

En el IFAI comprendemos que la discusión sobre el derecho de las personas a la protección de sus datos personales debe entenderse como producto de una ya longeva, pero también rica tradición liberal que busca dos aspectos fundamentales para las sociedades democráticas. Por un lado, acotar el poder del Estado y de los grupos, es decir, las corporaciones y las redes antisociales frente al individuo. En consecuencia, el tema central de las sociedades democráticas tiene que ser la protección del individuo partiendo del más débil y del más necesitado. Desde esta perspectiva, toda barrera que se imponga para impedir la vulneración del espacio privado es bienvenida y representa un avance civilizatorio.

Por otra parte, una de las razones de ser del Estado en regímenes democráticos es la construcción de espacios de libertad, protegidos para los individuos con la finalidad de que puedan desarrollar sus vidas con dignidad, integridad y autonomía.

En otros términos, los países de la región deben fijar su posición en esta materia para poder garantizar que todos los niños, niñas y adolescentes puedan hacer uso de la tecnología sin riesgo para su integridad física y moral. Si entendemos como sociedad, como instituciones garantes de la protección de la privacidad, pero también desde el sector privado la importancia de esta perspectiva de derechos, entonces estaremos en la ruta de una verdadera construcción democrática.

Dicho lo anterior, el presente compendio aborda a profundidad el tema de la protección de datos de niñas, niños y adolescentes en las redes sociales digitales a través de ocho ensayos con aproximaciones diversas. Entre los temas analizados se encuentran los antecedentes y la evolución del *Memorándum de Montevideo* a partir de la visión de libertades y derechos. Asimismo, aporta un análisis desde la perspectiva de género y su carácter transversal en la vida real y en consecuencia en el entorno digital, al tiempo que brinda herramientas para la protección del menor desde el anonimato con un balance entre el derecho a la libertad de expresión y la protección de la privacidad. El texto aquí presentado aborda desde la teoría y la práctica la protección en el entorno digital y muestra casos exitosos en la región.

En el IFAI estamos convencidos que este compendio brindará insumos indispensables para enriquecer el conocimiento y la comprensión del tema de la protección de datos personales en las redes sociales digitales, al tiempo de coadyuvar a su difusión y promoción, avanzando así en el camino hacia una sociedad plenamente democrática, que como tal, vela por el interés superior del niño.

Jacqueline Peschard Mariscal

Comisionada Presidenta del Instituto Federal de Acceso a la Información y Protección de Datos (México)

El enfoque de derechos en el "Memorándum de Montevideo"

Farith Simon Campaña[*]

La Web 2.0, en particular las redes sociales,[1] es una inestimable oportunidad para que niños, niñas y adolescentes accedan a información, expresen e intercambien opiniones, den a conocer sus creencias, socialicen, se asocien con otros con intereses similares, etc. Al mismo tiempo son espacios en los que podrían enfrentar situaciones que ponen en riesgo su integridad física, sicológica, social, sexual.

Algunos de los riesgos asociados al Internet que se han identificado son:[2] uso abusivo y adicción, vulneración de derechos de propiedad industrial o intelectual, acceso a contenidos inapropiados, interacción y acecho por otras personas y *ciberbullying*, *grooming* y acoso sexual, amenazas a la privacidad, riesgo económico y fraude,

[*] El autor es Doctor en Jurisprudencia y profesor de tiempo completo del Colegio de Jurisprudencia de la Universidad de San Francisco de Quito.

[1] Las redes sociales son "Plataformas de comunicación en *línea* que facilitan al individuo crear o unirse a grupos conformados por más usuarios. A través de ellas, el individuo intercambia información con [personas] de ideología, gustos, necesidades y problemáticas afines. [Son una forma de romper] el aislamiento de la mayoría. Dan popularidad al anónimo…integración al discriminado…" (Véase Lina Ornelas Núñez, "La Protección de menores en internet", febrero del 2010).

[2] Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres, *Observatorio de la Seguridad de la Información*, marzo, 2009, p. 13.

riesgos técnicos y *malware*, etc.

Muchas de estas amenazas pueden ser provocadas por los mismos niños, niñas y adolescentes que -como usuarios- pueden vulnerar derechos de otros, afectar la integridad personal, violentar la intimidad, transgredir derechos de propiedad, etc.

No podemos olvidar que niños, niñas y adolescentes nacieron en la "Sociedad de la Información", son *nativos digitales*. Un estudio del Observatorio para la Seguridad de la Información, de marzo del 2009, da cuenta de una sustancial diferencia entre el uso adulto y el de los niños, niñas y adolescentes, mientras los primeros usan el Internet con una finalidad, es decir –de acuerdo al estudio citado estudio- es "para algo". Los niños, niñas y adolescentes reportan un uso más natural, es decir , están en Internet, lo utilizan para estudiar para charlar o para escuchar música: "Internet constituye una herramienta básica de relación social e identidad".

El estudio citado demuestra que los adultos sobreestimamos la incidencia de algunos riesgos (ciberbullying, acoso sexual violación a la privacidad) y minimizamos los más frecuentes (riesgos técnicos), existiendo un elemento común entre adultos y niños, niñas y adolescentes: no saben cómo enfrentar las amenazas cuando se producen.

Un enfoque positivo del tema deja en claro que el acceso a las redes sociales en Internet son una increíble oportunidad para el ejercicio de los derechos y pueden contribuir al desarrollo integral de las personas menores de edad en las dimensiones que propone la CDN: físico, social, material, espiritual, moral, pero sin perder de vista las amenazas existentes para sí mismo o terceros.[3]

Esta nueva realidad ha hecho que se den varias iniciativas para encararla, desde aquellas de carácter global, como la de la Unión Internacional de Telecomunicaciones de las Naciones Unidas (en proceso de redacción); las de carácter regional como la Opinión 5/2009 del Grupo Europeo de Trabajo sobre el artículo 29, y las locales como las de Canadá o Brasil.

En éste contexto surge el Memorándum sobre la protección

[3] Artículo 27.1 "Los Estados Partes reconocen el derecho de todo niño a un nivel de vida adecuado para su desarrollo físico, mental, espiritual, moral y social".

de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, el *Memorándum de Montevideo*, que es el resultado del trabajo de un grupo de personas, algunas de ellas representantes de instituciones públicas y privadas como el Instituto de Investigaciones para la Justicia (II-Justicia), el Instituto Federal de Acceso a la Información de México (IFAI), la Agencia de Protección de Datos de Uruguay, la Agencia de Protección de Datos de Cataluña, la Agencia (Comisariado) de Protección de Datos de Canadá, la Secretaria Especial de Derechos Humanos de Brasil, UNICEF, el Instituto Interamericano de Derechos del Niño, así como jueces de infancia y académicos en tecnologías de la información, derechos humanos y derechos de la infancia y adolescencia, con el apoyo del Centro Internacional de Investigaciones para el Desarrollo de Canadá.[4]

En el *Memorándum* asumen un enfoque de derechos[5] al tratar los temas relacionados al Internet, particularmente la Web 2.0, teniendo como supuestos: (1) la tensión existente entre ejercicio de los derechos (autonomía progresiva) de las niñas, niños y adolescentes y el rol que deben asumir los adulto en la guía para el ejercicio de los derechos (protección especial);[6] (2) sin negar los riegos asociados a la Web 2.0 es claro que las personas que se encuentran fuera de estos espacios están expuestos a una nueva forma de analfabetismo y exclusión en la era digital, situación que acompaña, y acompa-

[4] Las recomendaciones fueron adoptadas en el marco del *Seminario Derechos, Adolescentes y Redes Sociales en Internet* (con la participación de: Belén Albornoz, Florencia Barindelli, Chantal Bernier, Miguel Cillero, José Clastornik, Rosario Duaso, Carlos Gregorio, Esther Mitjans, Federico Monteverde, Erick Iriarte, Thiago Tavares Nunes de Oliveira, Lina Ornelas, Leila Regina Paiva de Souza, Ricardo Pérez Manrique, Nelson Remolina, Farith Simon y Marías José Aveiga) realizado en Montevideo los días 27 y 28 de julio del 2009.

[5] El enfoque de derechos en el "…es un marco conceptual para el proceso de desarrollo humano que desde el punto de vista normativo está basado en las normas internacionales de derechos humanos y desde el punto de vista operacional está orientado a la promoción y la protección de los derechos humanos […]. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Preguntas frecuentes sobre el enfoque de Derechos Humanos en la Cooperación para el Desarrollo*, Naciones Unidas, Ginebra, 2006, p. 15.

[6] Artículo 5 CDN, "Los Estados Partes respetarán las responsabilidades, los derechos y los deberes de los padres o, en su caso, de los miembros de la familia ampliada o de la comunidad, según establezca la costumbre local, de los tutores u otras personas encargadas legalmente del niño de impartirle, en consonancia con la evolución de sus facultades, dirección y orientación apropiadas para que el niño ejerza los derechos reconocidos en la presente Convención".

ñará, a millones de niños y jóvenes que no tienen posibilidad de acceder a Internet y por esta vía a la información, diversión que puede proveer, así como estar al margen de un espacio para difundir sus ideas y opiniones, así como para exponerse a otras ideas y opiniones, esto implica reconocer las potencialidades de éste espacio brinda para el ejercicio del derecho a la asociación, la ejercicio de la libertad de expresión, etc.; y, (3) el reconocer el principio del ejercicio progresivo (autonomía progresiva) conlleva que cualquier clase de respuesta asuma las diferencias de edad y madurez en el universo infancia, por tanto la necesidad de respuestas diferenciadas, en las que existan márgenes claros en los que se puede identificar lo prohibido y lo permitido.

El *Memorándum* de manera categórica declara que su "referente normativo fundamental" es la Convención de las Naciones Unidas sobre los Derechos del Niño (CDN), a partir del hecho de que todos los países de la región la han ratificado y por tanto refleja un 'consenso' en la materia.[7]

A partir de este reconocimiento se puede identificar que el documento se sostiene en cinco principios, por tanto todas su recomendaciones se derivan de ellos, a saber*:*

1. Un enfoque de derechos que se refleja en lo siguiente:

   a. Reconocer que niñas, niños y adolescentes son titulares de todos los derechos humanos;[8]

   b. La incorporación del principio del ejercicio progresivo de

[7] En el lenguaje de la Opinión Consultiva OC-17/2002, de 28 de agosto del 2002, sobre la "Condición Jurídica y Derechos Humanos de los Niños" de la *Corte Interamericana de Derechos Humanos* la CDN refleja una *opinio iuris comunis* en los siguientes términos: "La Convención sobre los Derechos del Niño ha sido ratificada por casi todos los Estados miembros de la Organización de Estados Americanos. El gran número de ratificaciones pone de manifiesto un amplio consenso internacional (*opinio iuris comunis*) favorable a los principios e instituciones acogidos por dicho instrumento, que refleja el desarrollo actual de esta materia. Valga destacar, que los diversos Estados del continente han adoptado disposiciones en su legislación, tanto constitucional como ordinaria , sobre la materia que nos ocupa; disposiciones a las cuales el Comité de Derechos del Niño se ha referido en reiteradas oportunidades".

[8] Artículo 2.1. de la CDN, "Los Estados Partes respetarán los derechos enunciados en la presente Convención y asegurarán su aplicación a cada niño sujeto a su jurisdicción, sin distinción alguna, independientemente de la raza, el color, el sexo, el

   los derechos (la autonomía progresiva);[9]

   c. La obligación de tomar en cuenta las opiniones de niños, niñas y adolescentes en función de su edad y madurez;[10]

   d. El derecho a una protección especial en aquellas situaciones que resulten perjudiciales para sus derechos (en particular su desarrollo integral);[11] y,

   e. El reconocimiento del principio del interés superior, no como una cláusula que permite la discrecionalidad adulta para la restricción de los derechos, sino como una formula precisa que obliga a promover su respeto y garantía en un marco de estricta ponderación de los beneficios que las medidas que se tomen, especialmente aquellas de carácter restrictivo, tengan en los derechos.[12]

2. La responsabilidad compartida del Estado, la sociedad civil y la familia:[13]

   a. Asegurando un protagonismo de la familia en la guía del ejercicio de sus derechos.

idioma, la religión, la opinión política o de otra índole, el origen nacional, étnico o social, la posición económica, los impedimentos físicos, el nacimiento o cualquier otra condición del niño, de sus padres o de sus representantes legales".

[9] Artículo 5 CDN.

[10] Artículo 12 CDN, "1. Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño.

2. Con tal fin, se dará en particular al niño oportunidad de ser escuchado, en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional".

[11] Cuarto párrafo del preámbulo de la CDN señala, "Recordando que en la Declaración Universal de Derechos Humanos las Naciones Unidas proclamaron que la infancia tiene derecho a cuidados y asistencia especiales"; Artículo 3.2., "2. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con ese fin, tomarán todas las medidas legislativas y administrativas adecuadas".

[12] Artículo 3.1., "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".

[13] Artículo 5 CDN.

b. El rol específico del Estado.

c. Un reconocimiento del papel de la sociedad civil y los organismos multilaterales.

d. La responsabilidad de la "industria", como se ha llamado a los proveedores de los servicios, en generar soluciones a los problemas aquí planteados.

3. Un enfoque fundamentalmente preventivo y educativo, dejando en claro la necesidad de erradicar ciertas prácticas intolerables como la pornografía infantil en Internet.

4. Un definitivo "si" a la tecnología y los beneficios aparejados a ella, lo que se refleja en la necesidad de:

a. Extender los aspectos positivos de la Sociedad de la Información y Conocimiento (el Internet, las redes sociales);

b. Aceptar que es necesario enfrentar las prácticas perjudiciales, los riesgos y los impactos perjudiciales para el desarrollo y derechos de los niños, niñas y adolescentes.

5. Un reconocimiento de las *particularidades de género y de las provenientes de la rica diversidad cultural* en América Latina.

En el *Memorándum* se usa el principio del interés superior del niño de manera relevante, de hecho existen siete referencias al mismo a lo largo del documento.

La primera mención, y en mi opinión la más relevante, se hace en las llamadas "Consideraciones generales" en la que se deja en claro que debe priorizarse el interés de los menores de edad por sobre los de otros involucrados, ese interés se considera reflejado en la necesidad de que "…se guarde un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de esas herramientas que representan formas de ejercicio de sus derechos…"

Las otras seis referencias al principio aparecen a propósito de: a) las medidas de protección de los datos personales y de la vida privada de los menores de edad; b) al enfatizar la importancia de la educación para enfrentar los aspectos riesgosos de la Sociedad de la Información y Conocimiento; c) al recomendar que se instauren en los centros educativos mecanismos para resolver los conflictos

generados por el uso del Internet y las redes sociales; d) como "consideración primordial" para la "creación, reforma o armonización" normativa; e) al considerar que la responsabilidad civil extracontractual objetiva –para responder por los daños que se provocan en el Internet y las redes sociales digitales- se fundamenta en el interés superior, por ser una respuesta –se dice- "inmediata, eficiente y capaz de desincentivar los diseños peligrosos"; y, f) como "principio rector" para la formulación y desarrollo de las políticas públicas tendientes a regular las redes sociales digitales.

Todo lo anterior permite reafirmar que éste principio es considerado en su dimensión garantista, por tanto su aplicación se dirige siempre a favorecer los derechos, reflejándose esto en las recomendaciones que se formula en el documento y se agrupan en cinco ámbitos:

1. Recomendaciones en materia de prevención y educación de niñas, niños y adolescentes.

2. Recomendaciones para los Estados sobre el marco legal.

3. Recomendaciones para la aplicación de las leyes por parte del Estado.

4. Recomendaciones en materia de políticas públicas.

5. Recomendaciones para la industria.

A continuación un resumen general del contenido del *Memorándum* agrupado en los cinco aspectos antes indicados.

1. Recomendaciones en el ámbito de la prevención

A los niños niñas y adolescentes se les debe formar, en un lenguaje fácil, que permita la comprensión del espíritu de la protección de la vida privada de ellos y los demás, en: el uso responsable y seguro del Internet y las redes sociales digitales; en que el Internet es un espacio con normas y que las acciones allí tienen consecuencias, en particular debe hacérseles conocer que: la distribución de pornografía, el acoso, la discriminación, la promoción del odio racial, la difamación, la violencia son ilegales y penados por la ley; en el respeto a la vida privada, buen nombre e intimidad de terceras perso-

nas; en las posibles responsabilidades civiles, penales o administrativas derivadas del uso abusivo del Internet; debe formarse a niños, niñas y adolescentes en el uso responsable y seguro del Internet, en particular sobre las políticas de privacidad, seguridad y de alertas de las distintas redes y en la "incertidumbre" que rodea a la veracidad de la información en Internet y a buscar y discriminar las fuentes; y, debe recordarse que el uso de seudónimos es aceptado, siempre que estos no sirvan para el engañar o confundir sobre la identidad real, pero ello debe informarse sobre los riesgos de ser engañados sobre la identidad de la otra persona y los robos o la suplantación de identidad.

El proceso de promoción y educación sobre la Sociedad de Información y el Conocimiento, el uso seguro y responsable del Internet y las redes sociales debe ser permanente, para ello debe: incluirse en los planes educativos de todos los niveles; debe considerarse la participación de todos los involucrados en el diseño de los materiales, siempre tomando en cuenta las particularidades culturales y locales; la producción de materiales didácticos, especialmente audiovisuales, herramientas interactivas, etc.

Los docentes deben ser formados en estos temas. Las autoridades educativas –con el apoyo de las autoridades de protección de datos, académicos, organizaciones de la sociedad civil- deben asistirlos; debe establecerse –en los centros educativos- mecanismos para que los niños, niñas y adolescentes resuelvan los conflictos derivados del uso del Internet y las redes sociales (siempre con un espíritu didáctico y respetando todas las garantías).

Si se instauran medidas de control de las comunicaciones debería asegurarse que estas tengan como finalidad la protección y garantía de los derechos, ser adecuadas al fin perseguido y debe tomárselas siempre que no existan otras medidas menos restrictivas de los derechos.

2. Recomendaciones para el marco legal

Existe un lento avance del marco legal en relación al desarrollo nuevas aplicaciones y el avance de la tecnología, pero los vacíos y tensiones derivados de estos vacíos deberían ser enfrentados usando los principios constitucionales compatibles con estos temas.

Los cambios normativos que se impulsen deberían considerar lo siguiente: un principio que podríamos llamar 'espejo', es decir todo acción u omisión considerada ilegal en el mundo 'real' debe tener el mismo tratamiento en el mundo 'virtual'; debe asegurarse que los adolescentes puedan tener acceso a la información que existe sobre sí mismos, esto ya sea directamente o por medio de sus representantes.

En las regulaciones sobre los centros de acceso al Internet debería establecerse que estos utilicen mensajes de advertencia, filtros de contenido, etc.

Debe existir una normativa que asegure la protección de los datos personales y la aplicación efectiva de los mecanismos, dando prioridad a los niños, niñas y adolescentes.

3. Recomendaciones para la aplicación de la ley por parte de los Estados

Se reconoce el rol relevante que pueden cumplir los sistemas judiciales para asegurar el buen uso de Internet y la redes sociales. Experiencias recientes demuestran que pueden cumplir un doble rol: restaurar los derechos vulnerados; y, enviar un mensaje claro a ciudadanos y empresas sobre la voluntad aplicar las normas y los principios.

Para esto se debe garantizar: la existencia de procedimientos sencillos, ágiles y de fácil acceso, en donde estas causas se tramiten con prioridad; fomentar la especialidad en el juzgamiento de la protección de datos, promoviendo el desarrollo de la capacidad de los actores jurídicos; crear canales de comunicación para que niñas, niños y adolescentes puedan presentar denuncias; y, difundir ampliamente los fallos y crear bases de datos -anonimizadas- que los recopilen.

En el *Memorándum* se incentiva el uso de la responsabilidad civil extracontractual objetiva en esta materia, por considerar que es una respuesta inmediata, eficiente y capaz de desincentivar los diseños peligrosos y por ser el que mejor respeta el interés superior de niñas, niños y adolescentes.

4. Recomendaciones en materia de políticas públicas

En este ámbito en el documento se recomienda el establecimiento de: mecanismos de respuesta para las víctimas de abusos y sistemas de información para que niñas, niños y adolescentes tengan preocupaciones por su seguridad y derechos reciban asesoría y apoyo rápido; se deben elaborar protocolos para canalizar las denuncias sobre contenidos ilegales; crear mecanismos –nacionales e internacionales- para compartir y procesar información reportada sobre los eventos denunciados para establecer formas de protección temprana en base a los riesgos detectados; promover las sensibilización y divulgación de información pública sobre estos temas; promover la más participación en las acciones de difusión y sensibilización; impulsar el desarrollo de un conocimiento especializado en la materia y de investigación para formular políticas adecuadas.

5. Recomendaciones para la industria

En el *Memorándum* se reconoce la importancia central que tiene industria –proveedores de acceso, desarrolladores de aplicaciones y de redes sociales- en las medidas a tomarse en la prevención, en la cooperación con las autoridades y en las medidas de protección.

En el campo del manejo y protección de datos debe considerarse los siguiente: la protección de la vida privada debe ser la característica por defecto de todos los sistemas, las reglas sobre este tema deben ser explícitas sencillas y claras, en un lenguaje adecuado; los cambios de los perfiles de privacidad deben ser sencillos y gratuitos; los "parámetros de privacidad" deben estar disponibles siempre y advertirse sobre los que se han preseleccionado, asegurando que la opción sea la privacidad; no deben recopilarse los datos personales de niños y niñas; no debe permitirse la recopilación, tratamiento, difusión, publicación o trasmisión a terceros de datos personales, sin autorización expresa del titular.

En cuanto a la recopilación de datos personales se considera necesario: explicitarse los propósitos y finalidades para solicitar y recopilar cierta información personal, por ejemplo la edad para verificar que está por sobre la edad mínima permitida; precisar la manera en que se va a usar los datos de carácter personal; e, introducir sistemas de verificación de la edad.

Los sistemas deben tener formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios y no usuarios, en particular deben contar con: políticas accesibles sobre conservación de datos personales entre los que debe constar la eliminación , luego de un tiempo, de los mismos luego de que alguien desactive la cuenta; nunca se debe recopilar o mantener datos de no usuarios; las opciones para desactivar o suprimir cuentas deben ser visibles; debe informarse a los usuarios sobre las obligaciones de protección de la privacidad de terceros; debe impedirse la indexación de los datos personales de usuarios de redes sociales y prohibirse la indexación de información de niños y niñas.

De igual forma debe limitarse el acceso a los datos personales de parte de terceros proveedores de aplicaciones y evitar cualquier solicitud de datos no necesarios para el funcionamiento de las aplicaciones: los terceros solamente deberían acceder a los datos personales con autorización expresa del titular; las reglas de manejo de datos personales deben ser aplicados con independencia de lugar donde funciones los proveedores de redes sociales. Estas empresas deben fijar domicilio o representante legal en los países en los que tienen presencia significativa o por solicitud estatal.

Es necesario que todos los servicios establezcan filtros de seguridad y medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la disponibilidad y confidencialidad.

Para la erradicación de la pornografía infantil la industria debe comprometerse como mínimo a: notificar a las autoridades cualquier ocurrencia de pornografía infantil; preservar los datos necesarios y los contenidos de los usuarios por un plazo de seis meses; respetar de manera irrestricta las legislaciones nacionales sobre crímenes cibernéticos; reformular servicios de atención a clientes y usuarios para dar respuesta a todas las reclamaciones generadas por la creación de comunidades falsas u ofensivas; desarrollar tecnologías eficientes de filtrado e implementación de moderación para impedir publicaciones de pornografía infantil; crear herramientas de ayuda telefónica para brindar apoyo a niñas, niños y adolescentes y que las denuncias de estos sean procesadas de inmediato cuando exista indicios de pornografía infantil, racismo u otros crímenes de odio; retirar los contenidos ilícitos a requerimiento de las autoridades, manteniendo la información necesaria para la investigación judicial

de esos casos; desarrollar herramientas de comunicación con las autoridades competentes para la tramitación de denuncias; informar a los usuarios sobre los crímenes cometidos en las redes sociales digitales; desarrollar campañas de educación sobre el uso seguro y respetuoso del Internet, inclusive mediante la publicación de material impreso y audiovisual para ser distribuidos en los establecimientos educativos; y, establecer sitios de denuncia en línea de fácil acceso a niñas, niños y adolescentes.

En el *Memorándum* se recomienda la extensión de estas reglas a otros grupos vulnerables, la vulnerabilidad se relaciona al uso de datos sensibles que incluyen trabajadores, disidentes, personas con discapacidad y sus familias, inmigrantes e emigrantes, entre otros.

La importancia de estas recomendaciones es que asumen la complejidad de los temas asociados al Internet y a las redes sociales digitales desde una visión de derechos, reconociendo la responsabilidad que tienen los diferentes actores involucrados, todo esto sin negar el protagonismo que tienen niños, niñas y adolescentes.

En su redacción se ha privilegiado un enfoque pedagógico que permite a personas no familiarizadas con estos temas, especialmente los de naturaleza técnica, entender la complejidad y diversidad de los riesgos y de las medidas que pueden tomarse, por eso considero que la primera acción preventiva es difundir los contenidos del *Memorándum de Montevideo* y promover su discusión a todo nivel.

Impacto y evolución de las redes sociales digitales: libertades y derechos

Carlos G. Gregorio

Introducción

Es claro que Internet se ha desarrollado como un espacio propicio para la comunicación, el acceso a la información y el conocimiento, la trasparencia gubernamental, la expresión y todo ello rodeado de una atmosfera de creatividad e innovación. No por ello la satisfacción es plena, por un lado existen muchos aspectos sensibles y también la evolución futura es un enigma. La discusión que se hará entonces en este documento se concentrará —más que nada— en cómo las decisiones del presente perfilarán la evolución y optimización de las aplicaciones del futuro en un contexto de libertades y derechos.

Uno de los aspectos y expectativas básicas es que este desarrollo sea armonioso con el respeto de los derechos humanos, y en este sentido existen al menos dos aspectos preocupantes: evitar que se creen concentraciones de poder[1] y garantizar los derechos de las personas o grupos que devienen vulnerables como consecuencia de esta espiral

[1] La evolución histórica de los derechos humanos ha estado caracterizada por evitar las concentraciones de poder; comenzando por las monarquías absolutistas, los gobiernos de facto, y también los excesos de los gobiernos elegidos democráti-

de innovación.

Se comenzará por una discusión sobre los riesgos, fundamentalmente porque los logros y las nuevas oportunidades que se han generado son innegables. También es impensable una marcha atrás, solo se trata aquí de discutir los ajustes necesarios.

El marco legal en que ocurre esta evolución aparece como fundamental, porque el sistema de incentivos o regulaciones es el que determina la inversión y el que orienta la creatividad.

Es probable que hoy no sea posible —aun— contar con recomendaciones claras sobre cómo resolver los problemas, garantizar los derechos y maximizar las libertades; pero si es posible contribuir a este debate —en momentos muy acalorado y polarizado— con investigación, una visión ampliada y una identificación respetuosa de algunos consensos incipientes.

1. Riesgos

Los problemas y los riesgos suelen darse a conocer en estilo anecdótico, por casos particulares que resuenan en los medios, por críticas o denuncias. Pueden mencionarse dos categorías: los riesgos para la privacidad, intimidad o para la autodeterminación de los datos personales o la imagen; la otra categoría está definida por riesgos no virtuales, que no son nuevos, pero que se han recreado, o se ha modificado quiénes son ahora víctimas potenciales. Se incluyen los casos de fraude, robo de identidad y otros ciberdelitos, pero en este documento se trabajará con mayor profundidad la situación de los niños, niñas y adolescentes por su doble condición de nativos digitales y grupo vulnerable.

A partir de varios documentos recientes se ha puesto en evidencia la preocupación por los niños y adolescentes en el ciberespacio y la necesidad de complementar los marcos regulatorios, en particu-

camente. En este caso las empresas que hacen sus negocios en internet crecen e incrementan su posición de poder y el usuario está a merced de su oferta y a la aceptación de las condiciones de uso. Las leyes de trasparencia se aplican a los gobiernos, pero las empresas en internet se escudan en los secretos comerciales y paradójicamente se presentan como *servicio público*, que en una atmósfera de aparente gratuidad ofrecen servicios y aplicaciones.

lar la *Child Online Protection Initiative* del la Unión Internacional de Telecomunicaciones (del 18 de mayo de 2009); *Opinion 5/2009 on online social networking*, del Grupo Europeo de Trabajo del Artículo 29 (del 12 de junio de 2009) analizadas también en la perspectiva del *Acordo que põe fim à disputa judicial entre o Ministerio Público Federal de Brasil e a Google* (del 1 de julio de 2008); el *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. / Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.* (del 16 de julio de 2009).

Estos documentos han sido recientemente complementados por un documento elaborado en el Berkman Center for Internet & Society de la Harvard University[2] y por un estudio llevado adelante por iniciativa de la Comisión Europea.[3]

Estos documentos podrían resumirse en el reconocimiento de problemas, en particular para niños y adolescentes, generalmente ilustrados por casos particulares, y algunas veces presentados en forma dramática por los medios, que han motivado un llamado de atención que intenta recordar que vigencia de los derechos fundamentales (en particular la Convención de los Derechos del Niño) y la necesidad de una visión más amplia que incluya las nuevas tecnologías.

Por un lado se reconocen algunos riesgos intrínsecos pero se enfatizan algunos riesgos contextuales que se magnifican en particular en los países en vías de desarrollo.[4] La descripción de estos riesgos para los niños y adolescentes supone un conjunto de neologismos: *pharming, clickjacking*, gusanos, *cookies, ciberbullying, grooming y*

[2] Urs Gasser, Colin Maclay & John Palfrey, 'Working towards a deeper understanding of digital safety for children and young people in developing nations: an exploratory study by the Berkman Center for Internet & Society at Harvard University, in collaboration with UNICEF', (16 de junio de 2010).

[3] Sonia Livingstone, Leslie Haddon, Anke Gorzig & Kjartan Olafsson *et.al.*, 'Risks and safety on the internet: the perspective of European children (initial findings from the EU Kids Online survey of 9—16 years old and their parents', (21 de octubre de 2010).

[4] En un estudio reciente Gasser, Maclay y Palfrey analizan la vulnerabilidad *online* de los niños y adolescentes desde la óptica del país en que acceden a Internet. El enfoque del estudio acepta la existencia en las nuevas tecnologías de una multiplicidad de nuevas oportunidades para los niños y adolescentes, pero también hace

sexting.[5] Para los adultos uno de los riesgos que aun no reciben una respuesta adecuada es el de difamación y el uso indebido de la imagen.

Si hubiera que señalar algún factor reiterativo en la proliferación de estos riesgos, aparece inmediatamente el anonimato y la posibilidad que éste ofrece de suplantar una identidad, simular una edad o personalidad determinada y evadir toda responsabilidad. Al mismo tiempo se verá más adelante que el anonimato es un elemento clave en la evolución de Internet y que no puede —ni sería deseable— suprimirle *manu militari*.

En este orden de ideas nace también 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,*[6] *(Memorándum de Montevideo)* quizás interpretando que la protección de datos sería el primer paso de una garantía integral de derechos.

un exhaustivo análisis de los riesgos que se han percibido, destacando en forma reiterada que existen mucha información anecdótica y de casos puntuales que han ganado los medios, pero al mismo tiempo muy pocos datos obtenidos sistemáticamente. El estudio incluye una hipótesis subyacente que postula que no son iguales los riesgos para los niños y adolescentes de los piases industrializados que para aquellos de los países en vías de desarrollo. En esta vía de argumentación surgen una serie de consideraciones, entre ellas las que se refieren a "riesgos altamente contextuales" y a una sucesión de "historias trágicas en la cobertura de la prensa" que se complementan con la debilidad del estado de derecho y la falta de instituciones robustas. En definitiva la argumentación apunta a la necesidad de disponer de datos empíricos sobre victimización para justificar intervenciones en el balance de los derechos del niño con otros derechos fundamentales (y eventualmente con la libertad de expresión). Los riesgos para los niños y adolescentes en el uso de las nuevas tecnologías de información y comunicación no son nuevos riesgos, sino en su mayoría una redistribución de los riesgos preexistentes que ahora afectan diferentes poblaciones en distintos grados y fundamentalmente se expanden en una atmósfera de excesiva confianza, y por tanto, baja precaución y prevención. Por esa razón las políticas de seguridad son más críticas en los países en vías de desarrollo, dado que a los riesgos próximos se suman los globales, y las exiguas prevenciones locales reciben un magro apoyo desde el los países industrializados.

[5] Pablo Pérez San-José, Cristina Gutiérrez Borge, Susana de la Fuente Rodríguez, Laura García Pérez y Eduardo Álvarez Alonso, *Guía de introducción a la Web 2.0: aspectos de privacidad y seguridad en las plataformas colaborativas,* INTECO, (2011). Disponible en: http://www.inteco.es/file/pc8SqNjSy4wtSH7Apl5n5Q

[6] Ver www.iijusticia.org/Memo.htm

2. Niños, adolescentes y otros grupos vulnerables

Los riesgos son muy angustiantes para los niños y adolescentes; en un instante pueden pasar de un ambiente de juego y comunicación a estar siendo molestados o acosados por contenidos o personas que tratan de aprovecharse de ellos. Los niños y adolescentes suelen vivir estos eventos en soledad, pues temen que al confiarse en sus padres, la primera reacción de ellos será quitarles la conectividad. Aun cuando confíen en sus padres, el escenario más frecuente es que los padres no saben a quién acudir y que solo en muy pocos casos es posible, o remover los contenidos ofensivos, o identificar a los autores

En efecto, los nativos digitales han incorporado formas de socialización de las que les es muy difícil prescindir, pero las fallas en el sistema educativo y el halo de impunidad que rodea la intervención en Internet, han generado la situación en que niños y adolescentes son tanto víctimas como victimarios.

Las plataformas de relacionamiento (redes sociales digitales) son para los adolescentes un espacio obligado. En primer lugar porque son nativos digitales. También están siendo obligados a sociabilizar de ese modo; nuestros abuelos hacían nuevas amistades en la "plaza", nuestra generación en los *"shoppings"*, pero para los adolescentes de hoy es más difícil usar el espacio público, por la falta de seguridad y por las distancias en la nueva arquitectura de las ciudades.

Los intentos de solución son aun débiles: los filtros (o controles parentales) son ineficaces, no solo porque sería absurdo impedirles el acceso a las redes sociales, sino también si se considera que al mismo tiempo se desarrollan todos los días nuevos *proxis* para garantizar la libertad de información, que también anonimizan la conexión. Soluciones como la adoptada en otros medios de comunicación, como el horario de protección en la televisión, carecen de sentido en la red. Los filtros y el dominio .xxx recientemente aprobado luego de una larga discusión, podrían prevenir ciertos accesos, pero quedan muchas preguntas abiertas. También están las *helplines* y las *hotlines*.[7]

[7] Las *helplines* reciben llamadas, son un canal para que los niños u otros en su nombre, presenten situaciones conflictivas. Pueden ser desde adolescentes deprimidos

El *Memorándum de Montevideo* hace algunas recomendaciones que interpretan el consenso, como la de reforzar el sistema educativo con una marcada visión preventiva; pero también sugiere explorar líneas de intervención que tienen menor consenso —y que serán analizadas más adelante, pero que introducen la visión de una región (América Latina) que suma algunos factores difíciles de administrar (acceso y conexión predominantemente desde cibercafés, y un nivel mayor de riesgos contextuales).

Otros riesgos son poco claros e incluyen otros grupos vulnerables (como por ejemplo los trabajadores y los inmigrantes) y devienen de la disponibilidad de mucha información de carácter personal que es publicada pensando que se trata de una comunicación (grupal) privada pero que —de acuerdo a algunas reglas del sitio donde se colocan, pueden ser utilizadas con otras finalidades; los aspectos más preocupantes en este caso es la discriminación laboral que pueda generarse por la debilidad con que se garantiza el derecho al olvido. En este sentido —y ya entrando en un análisis quizás exageradamente especulativo— los juegos *online* son capaces de generar mucha información sobre la personalidad y podrían ser utilizados como un test psicológico en tiempo real; así rasgos personales como la agresividad o un excesivo detallismo podrían ser determinantes en la selección laboral, que podría desplazarse a buscar patologías antes que identificar habilidades.

3. Oferta de redes de relacionamiento

Es natural que un espacio tan dinámico e innovador con Internet esté matizado por una oferta difusa. Los ajustes de las aplicaciones ofrecidas son permanentes y están basadas generalmente en

a educadores sociales en un barrio que saben de un caso de abuso sexual y quieren informarse adónde derivar. Muchas situaciones de violencia se presentan a través de las líneas de ayuda. Ver *Child Helpline International* – www.childhelplineinternational.org y CAI Virtual (require registro previo) www.delitosinformaticos.gov.co. Las *hotlines* se dedican específicamente a identificar delitos en el ciberespacio. Deberían tener la tecnología y los conocimientos para ver dónde están alojados los contenidos, estudiar si ellos constituyen delito en esa jurisdicción, contactarse con las autoridades locales para que avancen, y en paralelo avisarle al proveedor para que baje los contenidos. Ver SaferNet Brasil – www.safernet.org.br y ASI México http://asi-mexico.org.

la aceptación y en las respuestas de los usuarios.

Muchas empresas (por ejemplo líneas aéreas), noticieros de televisión (por ejemplo CNN), ONGs e incluso instituciones del Estado,[8] difunden información y facilitan las participación en sus sitios en *Twitter* y *Facebook*: son usuales las frases "síganos en *Twitter*" o "estamos en *facebook*".

No se trata de establecer un relacionamiento, ni de ser amigo de una empresa gigantesca. En la práctica el mismo intercambio de información y las mismas expectativas podrías satisfacerse desde un sitio web, pero consultados algunos de directivos de empresas o de ONGs dijeron preferir redes sociales "porque los usuarios están más acostumbrados". Esto quiere decir que las redes sociales tienen un atractivo especial (que no es sociabilizar en red) sino ofrecer a los usuarios una lógica de contenidos preestablecida y común, una modalidad de participación e invitar a usar un lenguaje al que ya están acostumbrados. Para un usuario experimentado puede ser dificultoso encontrar en un sitio de gobierno, o de una empresa, o de una ONG la información que busca; debe enfrentarse primero a … ¿dónde están las cosas que busco? (puede ayudarse con el mapa del sitio, pero es muy probable que quede desilusionado, o con el buscador del sitio, y es probable que no resulte muy útil, y … luego de varios intentos se encuentra la información o abandona la búsqueda. ¿Qué ocurriría —entonces— con un usuario que habitualmente maneja solo su correo y su red social? … muy probablemente sienta que Internet es una gran complicación.

Entonces Facebook y Twitter (y no necesariamente otras plataformas de relacionamiento) ofrecen y tienen el monopolio de un lenguaje,[9] las cosas están donde ya se está habituado a encontrarlas … como estas redes son muy populares, es un terreno conocido para una población económicamente muy interesante. No parece muy racional que una oferta de relacionamiento se convierta en un estándar de lenguaje; sería entonces quizás más inteligente promover estándares para disponibilizar información en los sitios

[8] Ver facebook.com/us.embassy.montevideo

[9] Estas redes deben ser naturalmente monopólicas, pues quien está en una pequeña está incomunicado de la mayoría. Al inicio en algunos países los usuarios se caracterizaban por adherir a alguna red en particular —como *Orkut* en Brasil y la India, o *Tuenti* para los jóvenes en España— pero esta tendencia tiende a revertirse y ahora todos quieren estar en la "común".

web cuando está dirigida a usuarios en forma masiva, así cada sitio tendría dos opciones, la estandarizada y la "creativa" (esa versión que incluye "saltar la introducción" y un despliegue de imágenes y arboles de decisión para organizar la información).

Esto explica —en parte— el éxito de las redes sociales: redes dentro de la red, que mantienen cautivos a los usuarios. Que los mantienen dentro de un mercado complejo (el producto ofertado es solo la punta de un ovillo) y poco claro (se presentan como gratuitas, pero la moneda es la información personal — y cuanta más información mejor).

Del análisis de la oferta y de la demanda surgen algunas preguntas sobre las redes sociales —prefiriendo aquí el término plataformas de relacionamiento: ¿qué es comunicación? y ¿qué es comunicación grupal?, ¿cuándo existe expresión?, ¿cuándo la intensión es la asociación? ¿Cómo encontrar información, conocimiento u opinión pertinente? Y fundamentalmente si los diseños y aplicaciones ofrecidas, diferencian o confunden estas expectativas, y si privilegian u opacan los derechos y libertades que están detrás de cada una de ellas. ¿Existe libertad de diseño?

4. Libertades, derechos y políticas públicas

Existen varias expectativas predominantes en Internet, que se refieren a más libertad de expresión, acceso a la información, trasparencia y las posibilidades de comunicación y asociación.

Acceso a la información, conocimiento y trasparencia es una expectativa significativamente lograda. También existen logros para las posibilidades de comunicación interpersonal y grupal, con matices y criticas (hay quienes piensan que la comunicación es de contenido muy trivial —algunos dice que es mas cotilleo que relacionamiento; que los ciudadanos están sobrepasados de información pero mucho menos comunicados que antes, en fin este es el debate).

Sobre la libertad de expresión —quizás la expectativa mas sustantiva— se podría decir que está en desarrollo, con logros puntuales muy extraordinarios. Hay quienes dicen que si bien existen hoy muchas más posibilidades de expresarse, también se ha señalado

que es menos posible ser oído, producir impacto y generar transformaciones significativas. El impacto de una idea publicada en un artículo en un periódico de gran circulación —de lectura obligada— o difundida por televisión, no es igual a que aparezca en un *blog* que en la mayoría de los casos es conocido solo por quienes piensan igual y que es muy difícil de encontrar por la saturación de las búsquedas en Internet.

Dice Balkin, "las decisiones más importantes que afectarán el futuro de la libertad de expresión, no ocurrirán en el ámbito del derecho constitucional; ellas serán las decisiones sobre el diseño tecnológico, las regulaciones legislativas y administrativas, la formación de nuevos modelos de negocios, y las actitudes colectivas de los usuarios finales".[10] En consecuencia es posible inferir que la libertad de expresión debe ser repensada a la luz de la capacidad y potencialidad de internet.

Hoy uno de los incentivos que opera sobre los desarrollos y diseños de aplicaciones de relacionamiento se remiten a la sección 230 de la *Communications Decency Act* de los EE.UU. en la que los proveedores son inmunes frente a acciones judiciales por contenidos —denominada protección para el buen samaritano:[11] Section 230(c)(1) *"[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".*

En los EE.UU. la Primera Enmienda es determinante en este análisis. Rebecca Tushnet encuentra que la discusión teórica sobre la libertad de expresión se centra en la implicaciones de "enfocarse en quien habla" versus "enfocarse en la audiencia".[12] Por ejemplo Barron señala un profundo interés en proveer a los ciudadanos de un amplio acceso a puntos de vista conflictivos y a asuntos poco corrientes, no porque quienes tienen ideas disruptivas tengan dere-

[10]Jack M. Balkin, "The Future of Free Expression in a Digital Age" (January 29, 2009). *Pepperdine Law Review*, Vol. 36, 2008. Disponible en SSRN: http://ssrn.com/abstract=1335055

[11]www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

[12]Rebecca Tushnet, "Power Without Responsibility: Intermediaries and the First Amendment", 76, *Geo. Wash. L. Rev.,* 101 (2008). Disponible en SSRN: http://ssrn.com/abstract=1205674

cho a ser oídos, sino porque la sociedad tiene un especial interés en oírles.[13]

Estos argumentos son fundamentales al momento de discutir sobre los diseños de las aplicaciones de Internet en las que la libertad de expresión está en juego. Mientras que hoy existen diseños que facilitan expresarse, no tienen un desarrollo semejante aquellos que permiten encontrar puntos de vista conflictivos u opiniones en temas atípicos. O sea mientras que las plataformas de relacionamiento, y en particular los *blogs*, las posibilidades de comentar noticias y muchas más aplicaciones se abrogan (o autodefinen) como herramientas de libertad de expresión —y de hecho han incrementado la posibilidad de expresarse— simultáneamente se ha tornado mucho más complejo encontrar opiniones.

Continua Rebecca Tushnet: "una teoría de la libertad de expresión centrada en la audiencia, no puede aceptar que la Primera Enmienda es satisfecha por la no intervención del gobierno en el mercado … fundamentalmente porque las estructuras privadas que la ley habilita determinarán qué puede oír la audiencia y en qué manera puede responder".

Como operan entonces los mecanismos para oír: la primera respuesta es que este es el *rôle* de los buscadores —pero los buscadores más populares son cero-transparentes y en algunos casos abiertamente no neutrales.[14] Otros mecanismos se centran en el interés de los medios clásicos (prensa escrita y televisión) de motivar mecanismos de participación en línea, para seleccionar algunas intervenciones. Pero cualquier selección —hasta la más honesta y con intensión de neutralidad— no deja de ser una parte del discurso.

[13]Jerome A. Barron, "Access to the Press—A New First Amendment Right"*, Harv. L. Rev.,* (80), 1641, 1641, 1653–54 (1967).

[14]Los buscadores tienen una función esencial en el acceso a la información, sin embargo los algoritmos de búsqueda son un secreto industrial, y en la práctica no todos los sitios web están indexados. Usar un buscador eficientemente exige habilidades bastante desarrolladas, no esperables al menos en un ciudadano común. Mientras que la oferta de redes sociales es muy grande porque existe un rédito en términos de perfiles y datos personales, existe escasez de herramientas para encontrar información. La neutralidad de los buscadores puede evaluarse con un ejercicio muy simple: buscando un hotel por su nombre y ciudad, "normalmente" aparecen en los primeros resultados los sitios de los revendedores de habitaciones de hoteles (¿ … es que están en esas posiciones porque pagan por ellas?), y buscando cuidadosamente en la tercera o cuarta página aparece el "sitio web oficial" del hotel (normalmente si el hotel es pequeño y de pocos recursos).

Otros intentos apuntan a usar estadísticas sobre los comentarios en las redes sociales; por ejemplo dicen "la palabra más utilizada esta semana en *Twitter* ha sido …" … pero adaptando un antiguo refrán "aunque tú en la estadística estés presente, tu voz para la audiencia está ausente".

5. Expectativas y derechos en las plataformas de relacionamiento

Cuando el Grupo del Artículo 19 se preocupa por algunos aspectos presentes de las redes sociales: "Cuando el acceso a la información del perfil va más allá de los contactos elegidos, en particular, cuando todos los miembros que pertenecen al servicio de red social pueden acceder a un perfil o cuando los datos son indexables por los motores de búsqueda, el acceso sobrepasa el ámbito personal o doméstico. Del mismo modo, si un usuario decide, con perfecto conocimiento de causa, ampliar el acceso más allá de los «amigos» elegidos, asume las responsabilidades de un responsable del tratamiento de datos. En la práctica, se aplica entonces el mismo régimen jurídico que cuando una persona utiliza otras plataformas tecnológicas para publicar datos personales en Internet". Finalmente dice que aunque la *excepción doméstica* no se aplique debe establecerse un equilibrio entre la libertad de expresión y el derecho a la intimidad.[15]

Cabe preguntarse o inferir entonces que mientras no exista indexación de los contenidos y si el número de amigos es "razonable" el usuario no está "expresándose" sino "comunicándose". Es difícil de responder pero es una hipótesis muy fértil. No parece muy razonable que quien tenga una expectativa de expresión quiera voluntariamente limitar su audiencia y reducir la probabilidad de que su opinión sea encontrada (ciertamente si solo quiere evitar el acceso de quien puede perseguirle o discriminarle por sus ideas).

Este manto de optimismo bajo el cual se colocan derechos, expectativas y diseños no va más allá de un ejercicio de imaginación para desmitificar el concepto de que el mejor escenario posible para que las nuevas tecnologías evolucionen y se desarrollen sólo son las

[15]Por ejemplo en España la *Ley Orgánica de Protección de Datos* dice: "El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación: a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas".

reglas del mercado.

No huelga insistir, sin lugar a dudas desde la generalización de Internet una de las expectativas de impacto en las instituciones democráticas es que las aplicaciones en Internet producirían un notable incremento en el derecho a la libre expresión.[16]

Tabla 1. Aplicaciones sociales digitales.

	COMUNICACIÓN INTERPERSONAL	COMUNICACIÓN GRUPAL	EXPRESIÓN NO INTERMEDIADA	EXPRESIÓN INTERMEDIADA
DERECHOS EN EXPECTATIVA	derecho a la comunicación derecho al a privacidad de las comunicaciomes		libertad de expresión derecho a la imagen	
EJEMPLOS	teléfono	*Facebook* *Orkut*	*Twitter, blogs, wikileaks, YouTube,* "comente esta nota"	"medios" en su sentido clásico
	teléfono móvil correo electrónico			
CONTENIDOS Y ACCESO	no intervención de las comunicaciones sin orden judicial	sin indexación[17] *robots* identifican valoraciones a las reglas del sitio[18]	indexado (a veces con moderador que aplica las reglas del foro)	indexado (con editor responsable)
IDENTIFICACIÓN	identificador de llamadas IMEI - SIM card[19] teléfono público[20]	pseudónimo posible (criterio de aceptación de amigos)	pseudónimo posible	pseudónimo casi-imposible
AUDIENCIA	los interlocutores muchos	el grupo o los "amigos"	absolutamente todos	los lectores, televidentes, etc.
RIESGOS PARA LOS NIÑOS Y ADOLESCENTES	bajo	alto	medio	casi nulo

[16]La libertad de expresión implica dos derechos, *viz*. el derecho a la libre expresión, y el derecho a no expresarse, a quedarse en silencio y a retener la información propia.

[17]En realidad no es siempre así, dependiendo de la red social y del nivel de privacidad seleccionado el contenido puede ser indexado por los buscadores universales en Internet (*Google, Yahoo, Bing,* etc.).

[18]En muchas aplicaciones se incluyen *robots* que analizan contenidos privados con fines de enviar publicidad comercial, esto supone una disminución del derecho a los datos personales y a la privacidad de las comunicaciones. Su aceptación es discutible, pero su generalización abre también la posibilidad de utilizar estos robots para detectar situaciones de acoso, difamación o contenidos ilegales.

[19]El IMEI (*International Mobile Equipment Identity*) y la SIM card (*Subscriber Identity Module*) tienden a hacer que cada teléfono móvil pueda ser identificado (y asociado generalmente a una persona), en algunos países cambiar estos códigos es considerado un delito.

[20]Ciertamente el teléfono público abre la posibilidad de llamas totalmente anónimas

En efecto en los últimos años se ha observado una transformación positiva en la libre expresión de ideas y opiniones; pasando de un modelo intermediado por empresas característico del pasado, a un conjunto de aplicaciones en Internet que permiten la expresión y manifestación de ideas en forma directa (como los *blogs*, la posibilidad de comentar notas en los periódicos virtuales y en alguna medida algunas redes sociales como *Twitter*).

El balance de este proceso aun no es claro; si bien existen hoy muchas más posibilidades de expresarse, también se ha señalado que es menos posible ser oído, producir impacto y generar transformaciones significativas. El impacto de una idea publicada en un artículo en un periódico de gran circulación —de lectura obligada— o difundida por televisión, no es igual a que aparezca en un blog que en la mayoría de los casos es conocido solo por quienes piensan igual y que es muy difícil de encontrar por la saturación de las búsquedas en Internet.

Este análisis remite a una discusión de cuáles son las aplicaciones disponibles en Internet conocidas genéricamente como *redes sociales*, cómo son usadas (*i.e.* cuáles son las expectativas de los usuarios) y cuáles serían los derechos que intentan priorizar.

En algunas redes sociales la expectativa predominante de los usuarios podría definirse como "un mecanismo de comunicación grupal asincrónico". Por ejemplo en las entrevistas a los niños y adolescentes sobre quiénes ellos creen que leen sus contenidos en redes sociales y quiénes ven sus fotos, la respuesta inmediata es "mis amigos".

Otras redes sociales como *Twitter*, o los blogs tienen una clara expectativa de ejercitar el derecho a expresarse (aun cuando algunos crean cuentas cerradas sólo para sus amigos).

La dificultad de diseñar una aplicación (un "medio de comunicación" en el sentido amplio propio del contexto de Internet) que maximice al mismo tiempo la privacidad de las comunicaciones y la libertad de expresión parece difícil (o imposible), y es probable que las aplicaciones disponibles actualmente tengan aun pautas confusas

que genera cierto riesgo, sin embargo el bajo nivel de conflictos asociados hace este riesgo relativamente admisible, en particular porque quien recibe la llamada tiene el control suficiente para interrumpirla.

sobre cual expectativa satisfacen. En este sentido es clara la consternación del Grupo del Artículo 19 al ver que la "excepción doméstica" puede haber perdido sentido cuando se refiere a usuarios de redes sociales con varios miles de amigos, así como en la contradicción de la indexación en los grandes buscadores de los contenidos de las redes sociales.[21]

6. Sistema de responsabilidades

Una vez más, la expectativa de libertad de expresión es de alguna forma una prioridad. Pero qué hacer con las cosas que entran por la ventana … pornografía infantil, apología del delito, datos confidenciales y de seguridad nacional, difamación, uso indebido de la imagen, exposición de los niños y adolescentes a contenidos inadecuados, violentos, la explotación sexual, o a la pornografía, etc.

El enfoque tradicional del derecho es desarrollar un sistema de responsabilidades para reprochar y en la práctica disminuir los riesgos y proteger los derechos. Pero estando en medio la libertad de expresión el sistema legal ha evolucionado evitando convertirse en un mecanismo de represión o cesura indirecta. Por esa razón muchos países han eliminado las sanciones penales —con privación de libertad— para algunos delitos como por ejemplo el de difamación (muchas veces usado para perseguir a disidentes políticos).

En los medios clásicos (prensa escrita, radio, televisión) las responsabilidades estaban definidas con cierta claridad por la figura de editor responsable, pero con los nuevos "medios" en Internet, instantáneos, anónimos y ampliamente accesibles la dilución de la responsabilidad ha ampliado la posibilidad de expresarse pero también ha generado abusos y víctimas.

La responsabilidad penal se aplica en algunas legislaciones. El ejemplo más resonante y reciente es el caso *Associazioni Vivi-Down vs. Google Italy s.r.l.* en Italia, donde se han aplicado sanciones penales a cinco directivos de *Google* por la publicación en *YouTube* de

[21]Opinión 5/2009.

un video que ridiculiza a un niño con síndrome de Down (pero las penas de prisión previstas por la ley se han dejado en suspenso).[22] También en España se aplican multas a intermediarios y colaboradores necesarios, pero la cuantía de estas multas es muy baja.

El otro ejemplo muy interesante son las sanciones civiles aplicadas en Brasil. Por ejemplo en una decisión del Tribunal de Justicia del Estado de Rio de Janeiro, Brasil, un operador de telefonía móvil fue encontrado responsable por los daños morales a una clienta de la operadora que recibió insultos bajo la forma de mensajes de texto anónimos enviados a través del sitio web de la empresa.[23]

También pueden traerse a colación una serie de conflictos que en los últimos años se han observado en Brasil y que están vinculados al uso de la red social *Orkut*, y que han derivado en una serie de procesos judiciales penales y civiles.[24] Las primeras reacciones del Ministerio Público en Brasil fueron al descubrirse que se utilizaba *Orkut* para compartir imágenes de pornografía infantil, situación que fue sucesivamente investigada por la Policía Federal de Brasil. El gran número de delitos identificados en el contexto de *Orkut* y los procesos penales derivados de ellos llevaron a la empresa *Google* a firmar un acuerdo con el Ministerio Público Federal y con la organización SaferNet para colaborar —bajo pena de multas muy significativas— con las autoridades en la persecución de estos delitos.[25]

Paralelamente comenzaron en Brasil a generarse una serie de demandas civiles, la mayoría de ellas por difamación, derecho a la propia imagen y algunas por pornografía infantil en las que se demandaba a *Google* por los daños morales.[26]

[22]Ver la sentencia completa en: http://speciali.espresso.repubblica.it//pdf/Motivazioni_sentenza_Google.pdf

[23]Ver *C.M.P. vs. Nextel Telecomunicações Ltda* (18 de octubre de 2010) se afirma que el riesgo está en una falla en la prestación del servicio al usuario al permitir que cualquier persona envíe mensajes vía Internet sin identificarse, no ofreciendo así a los consumidores el nivel de seguridad al que tienen derecho. La condena (4.000 reales) es insignificante.

[24]La red social *Orkut* es propiedad de *Google* y tiene predominancia solo en Brasil y la India.

[25]Ver www.safernet.org.br/site/sites/default/files/TACgoogleMPF_0.pdf, *Termo de a ajustamento de conduta, entre La Procuradoria da Republica no Estado de São Paulo, Google Brasil Internet Ltda. e SaferNet Brasil* (2 de julio de 2008).

[26]Casos similares han sido decididos en el mismo sentido en Argentina -incluso

Existen algunas notas características en estos procesos judiciales: (1) se inician en juzgados de menor cuantía denominados en Brasil *Juizados Especiais*, sin formalidades, no requieren el patrocinio de un abogado y no existen costas judiciales. El damnificado presenta una demanda contra un usuario de *Orkut* que solo conoce por un *nickname* (pseudónimo o nombre de fantasía) y subsidiariamente contra *Google* solicitando que revele la identidad del usuario; (2) el juez libra una orden a *Google* para que informe la identidad del usuario detrás del nombre de fantasía bajo una pena de 5.000 reales por día mientras no satisfaga esta información.[27]

En primer lugar *Google* adujo que los usuarios aceptaban los tribunales de los EE.UU. al adherir como usuarios de *Orkut*; la respuesta de la justicia de Brasil fue que esa aceptación es nula y que la jurisdicción de los tribunales brasileños es irrenunciable. En segundo lugar *Google do Brasil* (a quien estaban dirigidas las demandas) argumentó ser solo una oficina de representación; la justicia brasileña respondió que el uso del nombre *Google* y su calidad de representación, así como la capacidad para recolectar los pagos de los servicios de publicidad la hacían solidariamente responsable, y por tanto podía ser desmanda.

En una importante cantidad de casos *Google do Brasil* no ha podido identificar a la persona física detrás de los perfiles, entonces los jueces condenaban a *Google do Brasil* a pagar los daños morales que rondan los 10.000 reales por caso.

unos años antes, como *S. M. y L. E. vs Jujuy Digital y Jujuy.com*- pero en un número relativamente mucho más pequeño. La diferencia radica en un mayor nivel de acceso a la justicia que existe en Brasil que justifica litigar por cuantías indemnizatorias significativamente bajas. Ver el caso *Protectora Asociación Civil vs. Facebook*, *Inc.* (decidido el 11 de mayo de 2010), www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=104 que trata de un grupo de adolescentes que creó un perfil en *Facebook* para convocar a sus compañeros de escuela a ausentarse un día determinado y concurrir a un espacio público a festejar su rebeldía, la decisión judicial se limita a ordenar a *Facebook* la remoción del contenido. En el mismo sentido *P. O. vs. Facebook Inc.* Pero en el caso de difamación de una figura pública, www.iijlac.org/jurisprudencia/components.php?name=Articulos&artid=107

[27]Esta es una multa media, hay algunas variaciones de un juzgado a otro; equivale a unos 2.800 dólares por día. No en todos los casos *Google do Brasil* es el demandado, también existen casos contra *Fotolog* y *Facebook* y contra personas físicas cuando son identificables.

En el momento de la redacción del *Memorándum de Montevideo* se entendió que ambos procesos en Brasil —civiles y penales— representaban una de las experiencias más interesantes en América Latina y que habían sido determinantes para la firma de los convenios de colaboración entre la empresa *Google* y las autoridades judiciales. Por esa razón se incluyó en el capítulo correspondiente a *Recomendaciones para la Aplicación de las Leyes por parte de los Estados* el siguiente párrafo:

> 10.1. …Se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales. Las sanciones judiciales por los daños derivados tienen la ventaja de ser una respuesta inmediata, eficiente y capaz de desincentivar los diseños peligrosos. Este tipo de responsabilidad civil se fundamenta en el interés superior del niño.[28]

Este párrafo permite traer algunos conceptos necesarios para analizar el marco regulatorio, por ello se tornan pertinentes las siguientes consideraciones: (1) la recomendación se limita a los casos en los que un niño o adolescente es víctima, y en este sentido se hace referencia explícita al interés superior del niño; (2) la frase desincentivar diseños peligrosos alude a responsabilidad por productos elaborados y no a una simple responsabilidad por contenidos.

En este sentido las más recientes decisiones judiciales en Brasil fundan su condena en un diseño peligroso (responsabilidad por productos elaborados) encontrado por los jueces en la aplicación *Orkut*, fundamentalmente al ver que viabilizan una anonimidad ab-

[28]Claramente inspirado en la *Declaración de Principios sobre Libertad de Expresión*, de la Comisión Interamericana de Derechos Humanos de la Organización de Estados Americanos (octubre de 2000): "10. Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas". [Aprobada durante el 108° Período Ordinario de Sesiones de la CIDH].

soluta, y en el hecho de que ésta es una actividad lucrativa para la empresa.[29]

Los argumentos de *Google* frente a las decisiones judiciales en Brasil se remiten a la sección 230 de la *Communications Decency Act* de los EE.UU. en la que los proveedores son inmunes frente a acciones judiciales por contenidos —denominada protección para el *buen samaritano*.[30] Sin embargo las condenas en Brasil son por la responsabilidad derivada de productos elaborados, aplicaciones que incluyen la posibilidad de operar en forma anónima, y no necesariamente por un contenido en particular; debe tenerse en cuenta adicionalmente que la Constitución Política de Brasil garantiza la libertad de expresión pero excluye el anonimato.

> Artigo 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: … IV — é livre a manifestação do pensamento, sendo vedado o anonimato; V — é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; …

Se dice también que un sistema de sanciones civiles podría crear una censura indirecta con la consiguiente pérdida de libertad de expresión. Sin embargo la cuantía de las indemnizaciones en Brasil es muy moderada y puede ser interpretada como un suave incentivo a mejorar las condiciones de seguridad de las aplicaciones y está muy lejos de ser un riesgo económico para la empresa —es más bien una parte mínima de la externalidad negativa que existe en toda industria.[31]

En España se han observado alguna variabilidad en la jurisprudencia, fundamentalmente por la introducción de concepto de

[29]Ver *R. S. B. v. Google do Brasil Internet Ltda.* Sobre el anonimato como una protección de quien ejerce su derecho a expresarse puede verse el caso *John Doe v. Cahill* 884 A.2d. 451, 456 (Del. 2005) donde el proveedor del servicio conoce pero no puede revelar la identidad del usuario hasta que medie una orden judicial. Sin embargo el anonimato al que se refieren los casos de *Orkut* se crea cuando un usuario en una red social puede crear su perfil en un ciber-café y operar en una forma tal que es imposible de identificar (anonimato irreversible).

[30]www.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html

[31]En Brasil el proyecto de ley del Marco Civil de Internet dice: Artículo 19. El proveedor de conexión a Internet no será responsable por daños derivados de los contenidos generados por terceros. Artículo 20. El proveedor de servicios de Internet sólo puede ser responsable por daños derivados de los contenidos generados por terceros si, después de intimado para cumplir orden judicial, no tomase medidas para, en el marco de su servicio y dentro del plazo establecido, tornar indisponible el contenido señalado como dañoso.

"cooperador necesario" que ha desplazado en algunos casos al de "conocimiento efectivo".[32] La mayoría de los casos de difamación o atentado contra el honor hay ido por la vía civil, solo ocasionalmente se ha acudido también a la vía penal, con resultados desiguales.[33] Por ejemplo el casos de la concejala del ayuntamiento de Santa Brígida, condenada por intromisiones ilegítimas al *honor* de tres personas por los comentarios que se publicaron al pie de varios de sus artículos: en el fundamento jurídico sexto *"Por todo lo expuesto, y sin perjuicio de lo que debe añadirse en el fundamento de derecho siguiente, procede la condena de la demandada, en cuanto que la misma es titular del blog en cuestión, la cual, evidentemente, pudo restringir o eliminar los mensajes que han sido objeto de análisis en el presente procedimiento evitando con ello su divulgación. A este respecto, es necesario indicar que no se conoce la persona concreta autora de los comentarios, debiéndose exigirse a la titular del blog donde se produce la difusión un deber de diligencia con relación a los mensajes que acceden al blog"*.[34] La sentencia fue revocada por la Audiencia de Gran Canarias y esta revocación declarada firme el 10 de marzo de 2011.[35]

En el caso Mafius se dice *"que el recurrente es el creador de la blog, determinando su temática, y responsable de su mantenimiento, que admite comunicaciones anónimas y, pese al indiscutible contenido ofensivo, que no podía ser ignorado, del comentario de 18 de abril decide su mantenimiento hasta fechas muy posteriores, tal proceder aparece como propio de la autoría por cooperación necesaria del artículo*

[32]Antoni Rubí Puig, "El requisito del 'conocimiento efectivo' en las SSTS, Sala Primera, de 9 de diciembre de 2009 y 18 de mayo de 2010", *Revista para el Análisis del Derecho* (www.indret.com).

[33]Miquel Peguera, *La administración de un foro no implica responsabilidad penal por los comentarios vertidos en él por terceros* (caso elcomentario.tv), (2009) — http://responsabilidadinternet.wordpress.com/2009/10/11/caso-elcomentario-tv/

[34]http://victoriacasas.blogspot.com/2009/02/se-acabo-paso-pagina.html

[35]http://victoriacasas.blogspot.com/2011/03/la-sala-declara-firme-la-setencia-por.html

28.b) del Código Penal. No se trata de coartar la libertad y sí, simplemente, de señalar que la libertad lleva aparejada la responsabilidad por el uso que se hace de la misma".[36]

En la vía civil en el caso *Ramoncín contra alasbarricadas.org* el Tribunal Supremo de Madrid establece una indemnización civil de 6.000 €, a los que hay que sumar 5.300 € de gastos judiciales.[37]

La moderación de contenidos de acuerdo con las reglas del sitio es tanto una posibilidad como una consecuencia de las reglas de responsabilidad.[38]

Sobre la responsabilidad de los buscadores se han suscitado algunos casos. La Audiencia provincial de Barcelona ha resuelto que los buscadores no violan la propiedad intelectual cuando hacen y disponibilizan un *cache* de un texto protegido.[39] Recientemente la Cámara de Apelaciones Civil de la Ciudad de Buenos Aires ha establecido que los buscadores no son responsables por los contenidos de los sitios que indexan.[40] Sin duda sentencias judiciales muy plau-

[36]Sentencia 96/2007 de la Audiencia Provincial de Madrid, Sección 3ª, de 26 de febrero de 2007. Sentencia del Juzgado de Primera Instancia e Instrucción núm. 5 de Arganda del Rey, de 30 de junio de 2006.

[37]Disponible en http://s.libertaddigital.com/doc/sentencia-del-supremo-que- condena-a-la-web-alasbarricadas-a-indemnizar-a-ramoncin-41912140.pdf En Italia la ley establece la responsabilidad objetiva: artículo 16 de la Legge 31 dicembre 1996, N. 675 – www.parlamento.it/parlam/leggi/96675l.htm y artículo 2050 del Código Civil.

[38]Para este procedimiento se ofrecen algunos prototipos como www.keepcon.com. Keepcon ha desarrollado una tecnología que es capaz de detectar los contenidos de riesgo según las reglas definidas por cada cliente. Se hace automáticamente y si algún contenido es dudosos se modera manualmente con otra herramienta informática para facilitar el trabajo: http://www.keepcon.com/esp/index.php Santiago Siri, uno de sus creadores de la herramienta www.meaningtool.com que es capaz de detectar las partes relevantes de un texto de internet, saber de qué trata un documento colgado en la Red e incluso "hacer interpretaciones políticas de los textos" o de los "sentimientos" con los que se ha escrito algo. Asegura Siri: "es la única posibilidad costo-efectiva de acompañar el crecimiento"; "necesitamos una brújula para orientarnos", "el sistema puede arrojar luz sobre un texto que con una lectura humana no llegaría"; el fin es "resolver la sobredosis de información que hay en internet"; "necesitamos una brújula para orientarnos"; "el sistema puede arrojar luz sobre un texto que con una lectura humana no llegaría".

[39]*Aleix P. L. vs. Google Spain*, 17/9/2008 – www.interiuris.com/blog/wp-content/uploads/sentencia_google.pdf

[40]*V. D. C. vs Google Inc. y Yahoo de Argentina S.R.L.* 11/8/2010 — www.diariojudicial.com/documentos/Agosto2010/Bandana_Google_Yahoo.pdf

sibles dado que los buscadores son absolutamente necesarios para navegar en Internet.

Pero si la tendencia es que los buscadores sean un negocio opaco y sin responsabilidad alguna, cuál será la tendencia futura de las capacidades de búsqueda. Si la libertad de expresión tiene una fuerte componente en el derecho a encontrar información, como los buscadores evolucionarán en este sentido.[41]

7. Tratamiento de la difamación en los EE.UU.

Las decisiones judiciales —publicadas— en los EE.UU. muestran un perfil diferente; normalmente se trata de alguien que estima que determinada información en un blog es difamatoria y pone en marcha el mecanismo establecido para identificar un responsable.[42] El tribunal pude ordenar o denegar la identificacion y para ello se han articulado estándares, fundamentalmente son precedentes relevantes los casos *Dendrite v. Doe* (New Jersey) y *Doe v. Cahill*, (Delaware).

[41]En este sentido una experiencia personal del autor puede dar una perspectiva interesante. Hace diez años y para entender como operaban los buscadores y su capacidad de hacer accesibles contenidos en forma totalmente neutral desarrolle un sitio web para mi perro (que se llama *Manchitotauro*) e inscribí ese sitio en la opción que los principales buscadores tienen para solicitar que se indexe un contenido. El sitio fue dado de baja el año pasado y durante diez años y pese a la insistencia el sitio de *Manchitotauro* nunca fue indexado. Simultáneamente desarrolle otros sitios con otros contenidos en el mismo servidor pero incluí enlaces a ellos en el sitio de mi institución, estos si fueron indexados pese a que no solicite la indexación. La pregunta es ¿existe responsabilidad por no indexar? ¿es censura?

[42]Por ejemplo, en *Rules on Civil Proceedings in the Trial Court, Rule 224. Discovery Before Suit to Identify Responsible Persons and Entities.* (a) Procedure. (1) Petition. (i) A person or entity who wishes to engage in discovery for the sole purpose of ascertaining the identity of one who may be responsible in damages may file an independent action for such discovery. (ii) The action for discovery shall be initiated by the filing of a verified petition in the circuit court of the county in which the action or proceeding might be brought or in which one or more of the persons or entities from whom discovery is sought resides. The petition shall be brought in the name of the petitioner and shall name as respondents the persons or entities from whom discovery is sought and shall set forth: (A) the reason the proposed discovery is necessary and (B) the nature of the discovery sought and shall ask for an order authorizing the petitioner to obtain such discovery. The order allowing the petition will limit discovery to the identification of responsible persons and entities and where a deposition is sought will specify the name and address of each person to be

Los proveedores de los servicios disponen normalmente de muy pocos elementos de identificación: los que provee el usuario como nombre, dirección de correo electrónico, quizás un teléfono o una dirección; y los que obtiene por medios tecnológicos basados en la conexión a Internet. Al ser conectividad predominante identificable es probable que existan muy pocos casos de anonimato irreversible. La actitud de los jueces —y los estándares definidos— tiende a proteger, y establecer los límites, de la expresión anónima.[43]

8. Abordajes para una evolución armoniosa —con los derechos y libertades— de las redes sociales

Ya se han presentado algunos abordajes legales clásicos —como el de la responsabilidad civil— pero han surgido también otras visiones sobre las que se propone edificar el futuro de Internet.

8.1. La neutralidad como abordaje

Internet es visto como un espacio propicio para extender las libertades, en consecuencia se propone que no debe hacerse ninguna intervención —o quizás mínima— en la red, esta es la opinión de un grupo significativo y es la visión predominante entre los usuarios —aun cuando evaden discutir o minimizan el tema de los riesgos. Por esta característica difusa la neutralidad suele expresarse en diferentes niveles y con diferentes consecuencias.

La neutralidad de la red ha sido materia legislativa en Chile por la Ley 20.453 del 18 de agosto de 2010:

> Artículo 24 H.- Las concesionarias de servicio público de telecomunicaciones que presten servicio a los proveedores de acceso a Internet y también estos últimos; entendiéndose por tales, toda persona natural o jurídica que preste servicios comerciales de conectividad entre los usuarios o sus redes e Internet: a) No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red.

examined, if known, or, if unknown, information sufficient to identify each person and the time and place of the deposition.

[43]Expresarse en forma anónima es una forma de garantizar a quien se expresa que no existirán represarías o discriminación, es también al mismo tiempo una forma de facilitar la difamación, invasiones sobre el derecho a la propia imagen, comisión de delitos —como el de pornografía infantil— o apología del delito, por citar los más frecuentes. Aquí es difícil establecer un balance al estilo de William Blackstone, que podría —por ejemplo— decir *"es preferible que 10 personas sean difamadas a que a una se le impida expresarse anónimamente"*. Cuando Blackstone dijo en 1769 *"para la ley, es preferible que diez culpables escapen a que un inocente sufra"* sentó las bases del equilibrio entre debido proceso y seguridad ciudadana. William Blackstone, *Commentaries on the Laws of England, Book the Fourth, Chapter the Twenty-Seventh: Of trial, and conviction.*

En Brasil existe un proyecto de ley denominado *Marco Civil para Internet en Brasil*:

> Artículo 2. El uso de Internet en Brasil se fundamenta en el reconocimiento de la escala mundial de la red, el ejercicio de la ciudadanía en los medios digitales, los derechos humanos, la pluralidad, la diversidad, la apertura, la libre empresa, la libre competencia y la colaboración, y observará los siguientes principios:
>
> I – Garantía de la libertad de expresión, comunicación y manifestación del pensamiento;
>
> II – Protección de la privacidad;
>
> III – Protección de datos personales, de acuerdo con la ley;
>
> IV – Mantenimiento y la garantía de neutralidad de la red;
>
> V – Preservación de la estabilidad, seguridad y funcionalidad de la red a través de medidas técnicas compatibles con las normas internacionales y fomentando el uso de mejores prácticas;
>
> VI – Preservación de la naturaleza participativa de la red.

Pero el proyecto de ley en Brasil no hace una definición de los alcances de la neutralidad, como en el caso de la ley chilena; otras definiciones como la de Julio Alonso: "que la inteligencia, los servicios se ponen en los extremos de la red, y la red en sí trasmite todo sin mirar ni jerarquizar ni priorizar". El problema radica en que la neutralidad tecnológica es un concepto en extremo difuso y polivalente, alguna de sus interpretaciones se asemeja a afirmar la

neutralidad ética característica de las leyes de la evolución biológica, y la aceptación que los individuos más débiles o las poblaciones menos adaptadas están destinadas a desaparecer en aras de un ideal evolutivo; escenario inadmisible en las sociedades humanas y desde una visión de derechos humanos.

Como refiere Justine Nolan "Hoy, la capacidad económica de las corporaciones transnacionales va mucho más allá de la capacidad económica de los países en las que ellas operan, y su músculo político es también mucho más grande que la habilidad de algunos Estados para regularlas efectivamente. Este poder debería estar acompañado de responsabilidad".[44]

Por su parte Hans Ulrich Buhl y Günter Müller afirman: "El problema real no es el 'ciudadano transparente' que está a la merced de un 'Estado controlador", sino en el hecho que ningún Estado en el mundo puede protegernos contra la amenaza de anarquía en la red. Por eso los grandes recolectores de datos como *Google, Facebook, Microsoft* y muchas más empresas parecen monitorear todo —y no existe aún un genuino guardián identificable".[45]

Entonces preocupa la existencia de concentraciones de poder en la red frente a la expectativa de que el centro de la evolución debe ser el ciudadano y él quien logre empoderarse.

Balkin considera que el *rôle* de los jueces es menor "estoy persuadido sobre la trayectoria de los futuros debates políticos, nuestra atención se desplazará crecientemente a cuestiones de diseño —tanto institucional como tecnológico— que están significativamente más allá de la competencia judicial.[46] También Balkin preconiza la "libertad de diseño" pero su afirmación se limita solo al contexto de los juegos en línea.[47]

[44]Justine Nolan, "With Power comes Responsibility: Human Rights and Corporate Accountability", *UNSW Law Journal*, Volume 28(3), 582. Disponible en SSRN: http://ssrn.com/abstract=1556443

[45]Hans Ulrich Buhl y Günter Müller, "The 'Transparent Citizen' in Web 2.0: Challenges of the 'Virtual Striptease'", *Business & Information Systems Engineering*, (4)2010, 203-206.

[46]Jack Balkin, "Media Access: A Question of Design", *George Washington Law Review*, 76, (2008), p. 933 – http://ssrn.com/abstract=1161990

[47]Jack Balkin, "Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds", *Virginia Law Review,* 90, (2004) – http://ssrn.com/abstract=555683

Todos estos argumentos llevan a preguntarse cuan neutrales pueden ser los operadores de Internet —manteniendo su modelo de negocios—, y cuáles serán los mecanismos, estímulos o incentivos para determinar una red en la que el poder este en manos de los ciudadanos, y se prevenga adecuadamente la victimización.

8.2. La educación como abordaje

El abordaje educativo —que concita uno de los mayores consensos— es aquel que ve como estrictamente necesaria una educación de los usuarios para prevenir los riesgos y para aprovechar al máximo las ventajas de la sociedad de la información y el conocimiento. Este abordaje está dirigido a todos pero fundamentalmente a los niños, niñas y adolescentes y de preferencia en la enseñanza regular. Existe una analogía interesante sobre este abordaje, se remonta a los años 60 en los que se generalizo la bolsa plástica y simultáneamente comenzaron a producirse muchos accidentes de muerte por sofocación —en particular en los niños entre 3 y 5 años. El tema fue una conmoción durante esos años, y se crearon muchas campañas de concientización y en el plano legislativo se reguló la colocación de mensajes impresos en las mismas bolsas plásticas. Hoy parece un tema superado, ni existen estadísticas con este tipo de accidente y —podría decirse— que la prevención de este riesgo fue inculturizada. Si debe decirse que se aprobaron algunas leyes —que aun están vigentes— por las que las bolsas plásticas utilizadas en juguetes y otros objetos que pueden estar al alcance de los niños debían llevar perforaciones. O sea este ejemplo muestra una combinación de educación y disminución del riesgo.

El *Memorándum de Montevideo* hace un fuerte llamado a establecer políticas educativas y no hace sino coincidir con otros documentos y con la tendencia mayoritaria.

Aunque la prevención y educación para el uso seguro y responsable es una recomendación que cuenta con amplio consenso en el concierto internacional,[48] no por ello es necesariamente una tarea

[48]Este objetivo fue incluido como Meta nº 24 en el *Plan de Acción sobre la Sociedad de la Información y del Conocimiento de América Latina y el Caribe* (eLAC2015) aprobado en la ciudad de Lima el 23 de noviembre de 2010 en la Tercera Conferencia Ministerial convocada por CEPAL.

sencilla en América Latina y el Caribe. Varios países de la región están embarcados en programas "un ordenador por niño",[49] pero estas políticas públicas no han sido acompañadas con la inserción en los programas regulares de enseñanza de educación para un uso seguro de las nuevas tecnologías. Este desfasaje está acompañado por la dificultad de capacitar a profesores y rectores, y por la falta de recursos económicos en los presupuestos educativos para atender estas necesidades. Existen ONGs en la región que ofrecen la realización de talleres de prevención en las escuelas, pero es una oferta externa y que debe ser pagada por las escuelas que las solicitan; esta modalidad incide diferencialmente en las escuelas privadas que disponen de recursos adicionales.

Si bien las políticas de responsabilidad social empresarial puede ser un recurso muy valioso para solventar al menos las etapas iniciales de generación de los contenidos educativos y la capacitación de los profesores, muchos operadores (de conectividad, de aplicaciones en Internet y de telefonía móvil) no muestran en la región los mismos estándares de responsabilidad social empresarial que ostentan en sus países de origen.

8.3. La identificación como abordaje

Dado que la causa principal de la mayoría de los riesgos es el anonimato —y la sensación de impunidad que se deriva de él— muchos piensan que es necesario incrementar los sistemas de identificación de los usuarios.

En primer lugar puede decirse que el anonimato irreversible,[50] es una ilusión. Si es posible si una persona cree una cuenta de correo electrónico en un ciber-café, a partir de ella cree una cuenta en una red social o hace un comentario a una nota en un periódico; si tiene un cuidado extremo en que su opinión esté escrita en un lenguaje neutro, sea tan sucinta como pueda ser, y además realice todo esto

[49]Varios países de la región están embarcados en programas "un ordenador por niño", el Plan Ceibal en Uruguay es el que está más adelantado.

[50]Ver Gabriela Mendoza Correa, *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*, (publicado en esta misma obra).

por única vez … probablemente su anonimato sea irreversible. Pero la dirección IP ya lo ubica geográficamente, el idioma utilizado y el tema abordado reducen el círculo; y su estilo de lenguaje aporta más información. Pero Internet tiene sus reglas de negocios, y la libertad de expresión —en particular la expresión anónima— no es un buen negocio.

En las aplicaciones teóricamente gratuitas de Internet —fundamentalmente las redes sociales— el negocio consiste en acumular información adjudicable a un perfil: cuanta más información se posea del usuario, más probable es encontrar una publicidad que le interese.[51] Pero más información implica la pérdida del anonimato irreversible, o sea las redes sociales y su modelo de negocio no son el espacio adecuado para expresarse anónimamente. Muchos periódicos tienen la posibilidad de "comentar una nota" en un diseño en el que el anonimato irreversible es mucho más real, aun así muchos periódicos han decidido no habilitar esta posibilidad para evitar los riesgos y porque tiene sus costos de moderación para retirar los comentarios que no cumplen con las reglas del sitio; o sea si bien es un producto interesante para los lectores es encarado siempre como un plus y no como el negocio principal.

Para ahondar en el análisis histórico se puede mencionar el caso *Dreiffus*: este caso comenzó en 1894 cuando un documento llamado el "*bordereau*" que contenía información militar francesa fue encontrado por el servicio secreto francés en un cesto para papeles en la embajada alemana; el documento fue analizado y se dijo haber identificado como autor al capitán del ejército francés Alfred Dreyfus, utilizando un proceso geométrico y probabilístico para analizar la caligrafía.[52] Enjuiciado por un tribunal militar, fue condenado a prisión perpetua y desterrado en la Isla del Diablo situada en la costa de la Guayana francesa. El caso mostró la debilidad del proceso judicial y fue un hito en la historia del antisemitismo.[53]

[51]Las redes sociales no necesitan identificar al usuario, solo necesitan un perfil completo; pero un perfil (que incluya fotos, vinculación a perfiles de amigos y muchos datos más) está a un paso muy pequeño de un proceso de individualización.

[52]F. Taroni, C. Champod, y P. Margot, "Forerunners of bayesianism in early forensic science", *Jurimetrics J.,* 38, (1988), pp. 183-200.

[53]Ver Jean Jaures, *Les Preuves* disponible en http://fr.wikisource.org/wiki/Les_Preuves y Émile Zola, *J'Accuse,* disponible en www.pitbook.com/textes/pdf/jaccuse.pdf

Este como otros casos muestran la permanente intensión de identificar y los riesgos que cualquier proceso de identificación encierra. También muestra que siempre se esconden otros intereses y prejuicios en cómo se identifica. Pero también muestran que la información preexistente se usa para triangular la identidad del autor de un texto, una hoja de caligrafía es nada comparada con miles de datos relacionales con que hoy contamos: contactos, amigos, correos recibidos y enviados, imágenes, direcciones IP, browser y muchas cosas más. Es la cantidad de información la que atenta contra el anonimato irreversible, pero también hay intentos de institucionalizar la identificación.

En agosto de 2010 Telefónica de España S.A. anunció la compra de la red social *Tuenti* con la intensión de expandir sus operaciones en Brasil, Argentina y otros países de América Latina, especialmente entre el sector de los adolescentes y los jóvenes. Esta noticia preanuncia y explica un cambio en la conectividad a Internet, que en América Latina migraría de la predominancia de los cibercafés a un uso de las redes sociales en forma concurrente desde los teléfonos móviles. Es muy probable que de concretarse este cambio, todo el escenario de riesgos se modifique. Al mismo tiempo podría ser una excelente noticia para los niños y adolescentes de América Latina y sus derechos; en particular porque *Tuenti* ha mostrado su compromiso con la legislación aplicable al firmar un acuerdo con la Agencia Española de Protección de Datos y también porque *Telefónica* ya cuenta con políticas de responsabilidad social en la región.

En alguna medida, en la mayoría de los países de América Latina, la conexión por teléfono móvil es identificable a una persona física, es decir que un perfil de red social quedará más probablemente identificado a un usuario que en la modalidad de acceso anterior.[54] Si se acepta que el anonimato absoluto y la suplantación de identidad en los espacios de chat, redes sociales y otras aplicaciones en Internet es una de las causas de vulnerabilidad de los niños y

[54]Recientemente el Tribunal Constitucional Alemán ha dictado una sentencia en la que ordena al legislador implementar una serie de requisitos para el almacenamiento de los datos de las telecomunicaciones y que los datos solo pueden ser utilizados para acciones judiciales si se sospecha un delito grave y utilizados en forma preventiva si existe un peligro concreto. También dice que no pueden guardarse registros de las llamadas a líneas telefónicas de ayuda que garanticen el anonimato.

adolescentes, un mayor nivel de identificación reducirá los riesgos para los niños y adolescentes, claro está esta reducción no será absoluta pues existen muchos teléfonos móviles no identificados —porque son antiguos o porque provienen de un mercado de segunda mano— pero esto es un aspecto factible de mejorar con la colaboración de las empresas y la responsabilidad de los usuarios. También algunos aspectos de diseño de las redes sociales podrían reducir los riesgos, como ser criterios más seguros para la aceptación de amigos.

También se sabe que los teléfonos móviles introducen nuevas vulnerabilidades para los niños y adolescentes; Gasser, *& al*. describen la modalidad de intercambio de imágenes —en algunos casos de pornografía infantil— a cambio de la acreditación de saldo, riesgo que ha sido también advertido en varios países de América Latina, que se suma a otros riesgos asociados a la cámara de video y a la posibilidad de trasferir archivos entre teléfonos móviles.[55] La responsabilidad civil también podrá ser aplicada, pero tendría un impacto positivo ya que son mucho más viables los diseños alternativos.

En definitiva existe una expectativa mayor de identificación en un contexto de comunicación pero no es así en plataformas para la expresión.

9. Problemas venideros

Sin duda el problema recién comienza y ni siquiera están claramente individualizados todos los problemas. ¿Cómo expandir un espacio de libertades con herramientas legales pensadas durante siglos para territorios delimitados? ¿Cómo conciliar el anonimato y resolver la protección del derecho al honor? ¿Cómo llevar a escala la educación y la prevención? ¿Cómo se prevendrá la discriminación injusta basada en perfiles?

[55]También la adhesión a redes sociales vinculadas a un teléfono móvil rompe la ilusión de gratuidad que hoy ostentan. Cuando en realidad en los servicios 'gratuitos' en Internet la moneda de pago son los propios datos personales y la aceptación de publicidad, esta nueva modalidad se parecería a incluir una aplicación más en el precio del paquete de conectividad.

El carácter comercial de la red es una fuerte perturbación. Supongamos un espacio de expresión anónima basado en el espíritu de generosidad que si existe en internet (al estilo de los *wiki*), quizás pueda ser muy poco atractivo en la medida que no está relacionado con una noticia —y entonces falla el derecho a oír (o encontrar). O si está relacionado con una pregunta (como hace CNN) … la formulación de la pregunta es ya una limitación. ¿Quién selecciona los comentarios que se mencionan, con qué criterio? ¿se hacen estadísticas y se busca representar las tendencias? ¿Las mayoritarias o las minoritarias? … en definitiva ¿Cómo se pasa de la nube a los medios clásicos? … o sea ¿solo los medios clásicos son la caja de resonancia adecuada de la expresión y las redes de expresión son solo un incremento en las "fuentes"?

La libertad de asociación es también otra incógnita. Sin duda la red ha mostrado resultados efectivos para movilizar y potenciar los movimientos sociales. Pero aun no se sabe a ciencia cierta cómo funciona y si puede ser controlado desde fuera.

La participación de los adolescentes —desprevenidamente— en algunas conductas delictivas (cyberbullying, pornografía infantil —incluyendo la auto-pornografía—, extorsión, entre otras) serán un desafío en muy poco tiempo para los sistemas de justicia penal de adolescentes. Un sistema que se caracteriza ya por su dificultad de atender al adolescente infractor respetando sus derechos, abusando de la internación e ignorando la necesidad de programas de inserción en libertad y basados en la comunidad.

Conclusiones

Obviamente estamos frente a un conjunto de expectativas, intereses y problemas que por el momento parecen inconciliables … también estamos frente a víctimas y grupos vulnerables, que están perplejos ante la inmovilidad de las instituciones de garantía de sus derechos. No se avizora hoy cual será la solución, pero es estimulante que continúe el debate y que se profundice el debate legal —desde un marco intelectual y académico.

Es muy probable que predomine el debate y la discusión sobre la libertad de expresión. Internet es un territorio en evolución,

por eso los estímulos e incentivos que existan hoy serán los que definan su futuro.

La inmunidad de la Section 230(c)(1) crea un importante incentivo hacia el desarrollo de herramientas de libertad de expresión, e inhibe otros mecanismos que podrían llevar hacia un equilibrio de derechos. En parte como afirma Bakin los diseños son claves para el futuro de internet, y para los diseñadores y proveedores es muy cómodo incluir la libertad de expresión en cualquier aplicación para evadir responsabilidades; diferenciar comunicaciones privadas, comunicaciones grupales y espacios de expresión no dejaría de garantizar la libertad de ; mientras exista una oferta razonable de aplicaciones para expresarse —incluyendo a la expresión anónima irreversible— las expectativas estarán satisfechas.

Quizás hoy no es posible optar por ningún abordaje en particular. Si hubiera silencio, aceptación y complacencia… tendríamos el futuro comprometido … se trata de mantener vivos los incentivos y los estímulos para quienes desarrollan y dan forma a Internet busquen un equilibrio saludable y armonioso.

El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a las redes sociales

Lina Ornelas[*]

Frente a la vulnerabilidad de los menores de edad y las nuevas formas de convivencia social a través de redes sociales digitales, el derecho no puede quedarse rezagado. Internet es un espacio lleno de oportunidades, es la puerta al mundo del conocimiento urbi et orbe, y uno de los nuevos roles del Estado consiste en el deber de esclarecer que no se trata de un espacio sin ley.

[…] la humanidad debe al niño lo mejor que puede darle.[1]

[*] La autora es Maestra en Derecho Europeo y Cooperación Legal Internacional por la *Vrije Universiteit Brussel*. Participó en la reunión celebrada en Montevideo, Uruguay convocada por el IIJusticia y el IDRC en 2009, para la elaboración del *Memorándum sobre la Protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes.* Se ha desempeñado como Directora General Adjunta de la Unidad para la Protección y Defensa de los Derechos Humanos en la Secretaría de Gobernación y ha publicado diversos artículos y textos en las materias de derechos humanos y protección de datos personales. Actualmente, ocupa el cargo de Directora General de Autorregulación del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) en México.

[1] V. Preámbulo de la Declaración de los Derechos del Niño de 1959. Documento de Naciones Unidas A.G. res. 1386 (XIV), 14 U.N. GAOR Supp. (No. 16), p. 19, ONU Doc. A/4354 (1959). Disponible también en: http://www.iin.oea.org/BADAJ2/pdf/Normativa%20ONU/Declaraci%C3%B3n%20de%20los%20Derechos%20del%20Ni%C3%B1o%201959.pdf

Introducción

El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto, a efecto de asegurar la autonomía de los individuos para decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias en dicha esfera personal. En particular, debe protegerse la información personal que niñas, niños y adolescentes proporcionan e intercambian en Internet a efecto de impedir su utilización inadecuada con fines distintos para los cuales ellos la proporcionaron.

Debe existir un balance entre asegurar la libertad de expresión en Internet de las niñas, niños y adolescentes sin que se afecte su dignidad como personas, ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un 'espacio privado' sin tener consciencia plena de que son observados y monitoreados.

La evidencia muestra que en todos los países, se han verificado afectaciones al desarrollo de la personalidad de menores de edad, derivado de las invasiones a los espacios de intercambio de información e imágenes que ellos frecuentan.[2] Los perfiles creados son almacenados, por lo que, aún borrada dicha información en Internet, ésta podrían ser utilizada en el futuro para conculcar otros derechos y libertades de los menores de edad ya en su vida adulta. Como afectación concreta podría ilustrarse a manera de ejemplo la no obtención de un determinado empleo por el hecho de que se conozcan cuáles eran sus gustos o preferencias durante la adolescencia.

Es innegable que hay un gran interés por conocer la información de los menores de edad. Internet ha facilitado dicha tarea. Distintos actores explotan la información de este sector de la población, tales como la industria, a la cual le interesa por ejemplo, conocer hábitos de consumo, lugares visitados y su frecuencia, composición y situación de las familias, entre otros aspectos.

[2]Véase los casos ilustrativos sobre el manejo de información personal de menores de edad en redes sociales digitales, expuestos como anexo al presente artículo.

Por su parte, los trasgresores de la ley -ahora también virtuales- obtienen información de los propios menores de edad o bien, la extraen por otros medios, para la comisión de delitos como el secuestro, trata o explotación sexual.

Es así como frente a la vulnerabilidad de los menores de edad y las nuevas formas de convivencia social a través de redes sociales digitales, el derecho no puede quedarse rezagado. Internet es un espacio lleno de oportunidades, es la puerta al mundo del conocimiento *urbi et orbe*, y uno de los nuevos roles del Estado consiste en el deber de esclarecer que no se trata de un espacio sin ley.

De tal forma que, el presente artículo se propone reflejar la evolución que han tenido los derechos humanos en general; el reconocimiento reciente de los derechos del niño y el nacimiento de un nuevo derecho fundamental a la protección de datos personales; las propuestas del Memorándum sobre la Protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes –*Memorándum de Montevideo*-, para concluir que los principios y derechos de protección de datos también resultan aplicables a este colectivo, y por tanto, el Estado debe actuar para garantizar su efectiva tutela.

1. Evolución de los derechos humanos

Los derechos humanos son normas que reconocen y protegen la dignidad de todos los seres humanos. Desde la perspectiva occidental de los derechos humanos, estos rigen la forma en que los individuos viven en sociedad, así como su relación con los gobiernos y las obligaciones que los gobiernos tienen para con ellos. De tal forma que, la ley de los derechos humanos obliga a los gobiernos a tomar una serie de medidas, y les impide tomar otras.

Los individuos, por su parte, también tiene responsabilidades: al hacer uso de sus derechos humanos, deben respetar los derechos de los demás. De esta forma, ningún gobierno, grupo o persona individual tiene derecho a llevar a cabo acto alguno que vulnere los derechos de los demás.

Los derechos humanos están basados en el respeto a la dig-

nidad y el valor de cada persona como individuo y también como miembro de la sociedad. La responsabilidad para asegurar que los derechos sean respetados, protegidos y satisfechos reside finalmente en los gobiernos nacionales.

Esta responsabilidad también concierne a otros elementos de la sociedad a nivel de las instituciones internacionales, pasando por la comunidad y llegando hasta los individuos en sus familias.

Sin embargo, cabe recordar que lo que hoy se conoce como *derechos humanos*, es producto de la evolución histórica reflejada en generaciones de derechos. Esto es, los derechos humanos para su comprensión, han sido divididos en categorías históricas que encuentran sus orígenes en el seno de la modernidad.

Esta perspectiva evolutiva de los derechos humanos implica el reconocimiento de nuevos derechos que intentan dar respuesta, en su gran mayoría, a las nuevas necesidades históricas. Por otro lado, otros suponen la redimensión de viejos derechos.[3] Tal como acontece en el fenómeno continuamente evolutivo de la sociedad tecnológica.

Derivado de lo anterior, ha prevalecido el reconocimiento de tres generaciones de derechos y se vislumbra una nueva oleada;[4] aquella relativa a los derechos en el ciberespacio y la libertad informática.[5] Así, cada etapa ha correspondido a un momento ideológico y social, con características particulares y rasgos diferenciadores, dependiendo de las necesidades de cada proceso evolutivo.

De tal forma que, la época burguesa del siglo XVIII marca el inicio de las etapas de los derechos humanos y, surgen de la Revolución Francesa como rebelión contra el Absolutismo. Las libertades individuales y la defensa de la persona se enmarcan como limitantes al poder público. Esta fase, se enfoca en la no injerencia con las libertades individuales y se configuran una serie de derechos relativos al aislamiento, tal como lo fue el derecho al honor, a la vida, a la integridad personal, así como el propio reconocimiento a la intimidad de la persona. Derecho que hoy, como consecuencia del desarrollo tecnológico y las nuevas formas de comunicación e información, ha sido necesario reformular en su alcance y contenido.

[3]Sobre el desarrollo y la concepción histórica de los derechos humanos, véase R.J. Vincent, *Human Rights and International Relations*, Cambridge University Press, Cambridge, 1999.

[4]La clasificación de los derechos humanos en tres generaciones fundamentales para su mayor entendimiento, fue propuesta por el jurista Karel Vasak en 1977, inspirado en los ideales de la Revolución Francesa. Introdujo el concepto de las 3 generaciones de derechos humanos en su conferencia para el Instituto Internacional de Derechos Humanos en Estrasburgo (1979). V. también Karel Vasak, *International Human Rights,* Vol. 1., Greenwood Press, San Francisco, EUA, 1982.

[5]Existe un reconocimiento más o menos generalizado del advenimiento de una cuarta generación de derechos humanos; al respecto, véase María Eugenia Rodríguez Palop, *La nueva generación de derechos humanos. Origen y justificación*, Dykinson-Universidad Carlos III de Madrid, Madrid, 2002.

En consecuencia, una segunda generación de derechos humanos, encuentra sus orígenes en las luchas sociales del siglo XIX y abarca hasta ya entrado el siglo XX. Estos movimientos reivindicatorios pusieron en tela de juicio la necesidad de contemplar el catálogo de derechos y libertades de la primera generación, con una segunda oleada de derechos económicos, sociales y culturales, incorporados en la Declaración Universal de 1948, debido a los cuales, el Estado de Derecho pasa a una etapa superior, es decir, a un Estado *Social* de Derecho.

Dicha fase, se enfoca en garantizar los derechos de participación a través del involucramiento activo de los poderes públicos mediante prestaciones y servicios; más aun, se incorpora de una tradición del pensamiento humanista y socialista. Si bien, los derechos de primera generación defendían a los ciudadanos frente al poder estatal, en esta etapa se exige cierto grado de intervención del Estado para garantizar un acceso igualitario a los derechos de carácter económico y social, esto es, para compensar las desigualdades naturales e inherentes a todo entorno social.

Cabe destacar que, en los años transcurridos desde la Declaración Universal de Derechos Humanos de 1948, y con mayor urgencia desde el final de la Guerra Fría, un gran sistema internacional de lo que se llaman instrumentos jurídicos del activismo y la defensa se ha desarrollado para proteger los derechos humanos. En otras palabras, se han integrado en los sistemas jurídicos de la gran mayoría de los Estados.

En consecuencia al intervencionismo estatal para garantizar los derechos de segunda generación, subyace la tercera generación encaminada a salvaguardar los derechos de la solidaridad. Esta generación encuentra su auge a partir de la segunda mitad del siglo XX, donde se

incentiva el progreso social y la calidad de vida de todos los pueblos.

Los derechos de tercera generación, son el resultado del reconocimiento de un nuevo contexto en el que surgen necesidades humanas particulares y donde las exigencias obligan a desarrollar nuevos derechos que garanticen el acceso universal a formas más avanzadas de ciudadanía y civilidad, de libertad y de calidad de vida.

Más aun, son indicios claros que el mundo cambió drásticamente en la última mitad del siglo XX. Transformación que es perceptible en nuestros días y que tiende a continuar. Está revolución se hace latente con mayor claridad en el uso de las nuevas tecnologías, vislumbrándose así el nacimiento de una cuarta generación de derechos humanos, en los que la universalización del acceso a la tecnología, la libertad de expresión en la web y la libre distribución de la información juegan un papel fundamental y son elementos esenciales para su definición.

Gracias al desarrollo generacional de los derechos y a su incorporación en el sistema jurídico internacional, hemos podido alcanzar la difusión global de los derechos humanos. Por lo tanto, hoy se da por sentado que corresponde al Estado y a la sociedad en su conjunto, el deber de proteger a cada individuo y garantizar el respeto irrestricto a los derechos humanos en su conjunto.

2. Evolución de los derechos del niño

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.

En 1945, la Carta de las Naciones Unidas estableció las bases de la Convención sobre los Derechos de los Niños -en adelante, la Convención- al exhortar a todos los países a promover y alentar el respeto por los derechos humanos y las libertades fundamentales *para todos*. Posteriormente, con la aprobación de la Declaración Universal de Derechos Humanos se reforzó la idea del respeto a los derechos de la infancia.

La segunda Declaración de los Derechos del Niño, adoptada en 1959, consagra algunos principios de fundamental importancia en esta materia. En particular, el derecho del niño a una protección especial se vincula con el concepto del desarrollo integral del niño, de su libertad y de su dignidad (v. Principio 2).

Posteriormente, con la Declaración de los Derechos del Niño y la consiguiente Convención, se establecen los derechos y obligaciones para asegurar el respeto irrestricto de la infancia.[6] Este último es reconocido como el instrumento internacional por excelencia para la protección de la infancia.

La Convención es el tratado internacional que ha sido más ampliamente ratificado en la historia de las Naciones Unidas. Ha sido ratificada por 192 países desde que la Asamblea General de las Naciones Unidas la aprobó de manera unánime en noviembre de 1989.[7] Si bien, es una Convención articulada *ad hoc* para la protección de la niñez - pues se concluyó que los menores de 18 años precisan de cuidados y protección especiales-,[8] también es cierto que, está fundamentada en otros instrumentos internacionales como la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales.[9] De tal forma que

[6]A este respecto, cabe recordar que las declaraciones son manifiestos con intención moral y ética, pero no son instrumentos jurídicamente vinculantes. El marco internacional de derechos humanos se fortaleció con pactos o convenciones, que tuvieran todo el peso de la ley internacional. Para mayor abundamiento sobre las diferencias de fondo entre pactos, convenciones y otros instrumentos internacionales, V. Alejandro Anaya Muñoz, *et. al., Glosario de términos básicos sobre derechos humanos*, Comisión de Derechos Humanos del Distrito Federal, Universidad Iberoamericana Ciudad de México, México, 2005.

[7]La aprobación final de los Estados Miembros de las Naciones Unidas se produjo después de que la Asamblea General de las Naciones Unidas aprobara de forma unánime el texto de la Convención sobre los Derechos del Niño el 20 de noviembre de 1989. La Convención se transformó en un documento jurídicamente vinculante en septiembre de 1990, después de su ratificación por 20 Estados.

[8]El Artículo 1 de la Convención establece que para los efectos de esta se entenderá 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".

Disponible en la página oficial del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, en el vínculo: http://www2.ohchr.org/spanish/law/crc.htm

[9]La Convención en su Preámbulo hace referencia a otros instrumentos internacionales. Se hace mención, no solo a las Declaraciones de los Derechos del Niño de

la normatividad internacional sobre derechos humanos contempla dentro del término *niño* tanto a las niñas y niños como a los adolescentes.

Es de hacer notar que el Preámbulo de la Convención reitera una frase contenida en el Preámbulo de la Declaración de 1959, que reza a la letra: "el niño, por su falta de madurez física y mental, necesita protección y cuidado especiales, incluso la debida protección legal […]".[10]

La Convención además de estar fundamentada en la Declaración de 1959 y otros instrumentos internacionales ya mencionados, está basada en diversos sistemas jurídicos y tradiciones culturales, además se compone de normas y obligaciones. Estas normas básicas -denominadas también derechos humanos- establecen derechos y libertades mínimas que los gobiernos deben cumplir y, se basan en el respeto a la dignidad y el valor de cada individuo, independientemente de su raza, color, género, idioma, religión, opiniones, orígenes, riqueza, nacimiento o capacidad.[11]

Cabe mencionar que la Convención es el primer instrumento jurídicamente vinculante que incorpora toda la gama de derechos humanos: civiles, culturales, económicos, políticos y sociales. En 54 artículos y dos Protocolos Facultativos,[12] se definen los derechos básicos que deberán disfrutar todos los niños y niñas inherentes a su dignidad humana y desarrollo armonioso. De tal forma que,

1924 y 1959, a la Carta de las Naciones Unidas, a la Declaración Universal y a los dos Pactos Internacionales, sino también a las Reglas de Beijing para la administración de justicia de menores, a la Declaración de 1986 sobre los principios sociales y jurídicos relativos a la protección y el bienestar de los niños, y a la Declaración de 1974 sobre la protección de la mujer y el niño en estados de emergencia o de conflicto armado.

[10]V. *Derecho Internacional de los Derechos Humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano,* Oficina de Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Bogotá, 2004, p. 796.

[11]La Convención define los derechos humanos básicos que disfrutan los niños y las niñas en todas partes: el derecho a la supervivencia, al desarrollo pleno, a la protección contra influencias peligrosas, los malos tratos y la explotación, y a la plena participación en la vida familiar, cultural y social. Asimismo, protege estos derechos al estipular pautas en materia de atención de la salud, la educación y la prestación de servicios jurídicos, civiles y sociales.

[12]La Asamblea General aprobó en 2000, dos Protocolos Facultativos de la Convención

la Convención es un documento moderno que refleja una nueva visión sobre la infancia, como seres humanos y *titulares* de sus propios derechos.[13]

Al ser un instrumento internacional ratificado por los Estados, éstos se comprometen a cumplir con un código de obligaciones vinculantes a favor de la infancia. Al aceptar las obligaciones -mediante su ratificación o adhesión-, los gobiernos se comprometen a proteger y asegurar los derechos de la infancia y aceptan que se les considere responsables de este compromiso ante la comunidad internacional. En consecuencia, los Estados parte de la Convención están obligados a llevar a cabo todas las medidas y políticas necesarias para proteger el interés superior del niño y,[14] son vigilados por el Comité de Derechos del Niño -órgano de expertos independientes que supervisa la aplicación de la Convención y los dos Protocolos, por sus Estados partes-.

En este tenor, es la sociedad en su conjunto quien debe asegurar su cumplimiento como una obligación jurídica, un imperativo moral y una prioridad en materia de desarrollo. Se entiende que es labor del Estado, la sociedad y la familia -cada uno en su ámbito de competencia- hacer cumplir las disposiciones estipuladas en la Convención. Las normas y los principios que se articulan en la Convención solamente pueden convertirse en realidad cuando sean respetados por todos, en la familia, en las escuelas y en otras institu-

que ofrecen más detalles y amplían las obligaciones del tratado original. Estos son: Protocolo Facultativo sobre la participación de los niños en los conflictos armados y Protocolo Facultativo sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

[13]Si bien es cierto, cuestionar los derechos de la niñez en la actualidad es considerado como *cuasi* herejía, cabe mencionar que existen argumentos en contra de la universalización de la Convención, sustentados en argumentos pluralistas donde normas globales encuentran dificultad aplicativa a culturas diversas. Esto es, existe un consenso internacional sobre el interés de la niñez lo cual no significa que exista un consenso sobre las políticas más adecuadas a implementar en beneficio de los niños. A mayor abundamiento sobre este debate, véase Vannesa Pupavac, "The Infantilization of the South and the UN Convention on the Rights of the Child", *Human Rights Law Review*, University of Nottingham, Centre for Human Rights, marzo, 1998. Para una perspectiva más general, véase Simon Caney y Peter Jones (eds.), *Human Rights and Global Diversity*, Frank Cass Publishers, London, 2001, pp. 27-77.

[14]Este principio es conocido como 'primacía del menor', al reconocer la importancia de medidas legislativas para el reconocimiento del *interés superior* del niño

ciones que proporcionan servicios a la niñez, en las comunidades y en todos los niveles de la administración pública.

La Convención ofrece una visión del niño como individuo y como miembro de una familia y una comunidad, con derechos y responsabilidades apropiadas para su edad y etapa de desarrollo. A este respecto, vale la pena mencionar que según la Convención, son los padres quienes tienen la responsabilidad primordial tanto de la crianza de sus hijos como de la satisfacción de las necesidades que permitan su sano desarrollo.[15] En la medida en que los padres, no estén en condiciones de cumplir con estas responsabilidades por sus propios medios, el Estado tiene el deber de apoyarlos –v. arts. 18.2 y 27.3–. Esta relación de co-garantes es reafirmada por el artículo 3.2. que establece a la letra lo siguiente:

> 2. Los Estados Partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con este fin, tomarán todas las medidas legislativas y administrativas adecuadas.

De tal forma que, en la medida que los padres no cumplan sus obligaciones a cabalidad, las autoridades tienen el derecho y el deber de intervenir para proteger los derechos del niño. En lo po-

como idea que debe orientar toda legislación en la materia. Encuentra sus orígenes en el artículo III de la Declaración de Ginebra de 1924, misma que consagra al niño como objeto de protección y sin protagonismo propio, a diferencia de las declaraciones y convenciones subsiguientes, donde se visualiza al niño como *sujeto* de derechos.

[15]A este respecto, el artículo 18, fracción 1 señala lo siguiente:

> 1. Los Estados Partes pondrán el máximo empeño en garantizar el reconocimiento del principio de que ambos padres tienen obligaciones comunes en lo que respecta a la crianza y el desarrollo del niño. Incumbirá a los padres o, en su caso, a los representantes legales la responsabilidad primordial de la crianza y el desarrollo del niño. Su preocupación fundamental será el interés superior del niño.

Por su parte, el artículo 27, fracción 2 establece lo que a continuación se indica:

> 2. A los padres u otras personas encargadas del niño les incumbe la responsabilidad primordial de proporcionar, dentro de sus posibilidades y medios económicos, las condiciones de vida que sean necesarias para el desarrollo del niño.

Disponible en la página oficial del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, en el vínculo siguiente: http://www2.ohchr.org/spanish/law/crc.htm

sible, la intervención consistirá en dar a los padres la orientación y el apoyo necesarios para superar los problemas que afectan la forma como cumplen estos deberes.

En este sentido, la Convención prevé disposiciones que abarcan derechos y libertades civiles, el entorno familiar, la salud básica y el bienestar, la educación, recreación, las actividades culturales y las medidas especiales necesarias para su protección.

En lo relativo a los derechos, la Convención establece principios fundamentales como la no discriminación, el derecho a la supervivencia, al desarrollo y la opinión del niño. Asimismo, establece como principio básico contemplar en todo momento el *interés superior del niño* como consideración primordial en todas las medidas y decisiones que le atañen, y debe utilizarse para resolver cualquier confusión entre los diferentes derechos.

En particular, tomar en consideración los puntos de vista de los niños y las niñas se refiere a la importancia de escuchar y respetar su opinión en todas las cuestiones relacionadas con sus derechos. De ahí que la Convención ha exhortado a los países a promover una participación activa, libre y significativa de la infancia en las deliberaciones para tomar decisiones que les afecten.

Cabe destacar, para efectos del presente análisis, el artículo 16 de la Convención establece el derecho y obligación a la protección del niño, por ministerio de ley, y a letra dispone lo siguiente:

> 1. Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación.
>
> 2. El niño tiene derecho a la protección de la ley contra esas injerencias o ataques.[16]

Por otra parte, la participación de la niñez constituye un aspecto con grandes potenciales en el vasto derecho de la infancia. También en esta área la Convención ha incorporado las bases para una profunda transformación cultural, introduciendo el principio de la autonomía progresiva de la infancia, tal como se consagra en

[16]Disponible en la página oficial del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Ibíd*.

el artículo 12.[17]

Asimismo, en el artículo 19 se establece la obligación del Estado a proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo custodia de los padres. A la letra señala lo siguiente:

> 1. Los Estados Partes adoptarán todas las medidas legislativas, administrativas, sociales y educativas apropiadas para proteger al niño contra toda forma de perjuicio o abuso físico o mental, descuido o trato negligente, malos tratos o explotación, incluido el abuso sexual, mientras el niño se encuentre bajo la custodia de los padres, de un representante legal o de cualquier otra persona que lo tenga a su cargo.
>
> 2. Esas medidas de protección deberían comprender, según corresponda, procedimientos eficaces para el establecimiento de programas sociales con objeto de proporcionar la asistencia necesaria al niño y a quienes cuidan de él, así como para otras formas de prevención y para la identificación, notificación, remisión a una institución, investigación, tratamiento y observación ulterior de los casos antes descritos de malos tratos al niño y, según corresponda, la intervención judicial.[18]

Por su parte, en el marco interamericano sobresalen el Pacto Interamericano de Derechos Civiles y Políticos y la Convención Americana, que reconocen el derecho del niño a "las medidas de protección que su condición de menor requiere". Si bien, la normativa interamericana no contempla una definición explícita del *niño*, el artículo 4.1. de la Convención Americana precisa que el derecho

[17]El Artículo 12 de la Convención de los Derechos de los Niños, establece a la letra lo siguiente:

> 1. Los Estados Partes garantizarán al niño que esté en condiciones de formarse un juicio propio, el derecho de expresar su opinión libremente en todos los asuntos que afectan al niño, teniéndose debidamente en cuenta las opiniones del niño, en función de la edad y madurez del niño.
>
> 2. Con tal fin, se dará en particular al niño oportunidad de ser escuchado en todo procedimiento judicial o administrativo que afecte al niño, ya sea directamente o por medio de un representante o de un órgano apropiado, en consonancia con las normas de procedimiento de la ley nacional.

Disponible en la página oficial del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, *Ibíd*.

[18]*Ibíd*.

a la vida "estará protegido por la ley y, en general, a partir del momento de la concepción".[19] Asimismo, en el artículo 19 relativo a los derechos del niño, se lee:

> 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.[20]

Esto es, la Convención Americana sigue lo establecido en la Convención al establecer que los niños y niñas necesitan protección especial precisamente por *ser* niños, y por lo tanto dependientes y potencialmente vulnerables.

Ahora bien, resulta pertinente señalar que pese a ser un tratado vinculante para los países que lo han ratificado, la Convención es un instrumento legal relativamente joven y en proceso de implementación en todos los Estados miembros.

De tal forma que, veinte años después de la aprobación de la Convención puede afirmarse que su implementación en América Latina continúa siendo un proceso dinámico y continúo no solo en su relación con las reformas legales y modelos institucionales, sino también respecto a cualquier situación nueva que pueda afectar directa o indirectamente la vida o libre desarrollo de los niños, niñas y adolescentes –tal es el caso de las tecnologías del conocimiento y la información-.

3. Un nuevo derecho fundamental: la protección de datos personales

Una vez que se ha abordado la evolución de los derechos humanos, conviene puntualizar que 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

[19]Disponible en la página oficial de la Organización de Estados Americanos, en el vínculo siguiente: http://www.oas.org/Juridico/spanish/tratados/b-32.html

[20]*Ibíd*.

un haz de facultades concretas. Por tanto, se trata en sí mismo de un derecho activo.[21]

Diversos instrumentos internacionales reconocieron el derecho de toda persona a no ser objeto de injerencias en su vida privada o familiar.[22] Aunado al desarrollo normativo y los avances científicos y tecnológicos, surge en Europa el germen y acuñación del derecho a la protección de datos como se desarrolla en líneas subsiguientes.

En 1967 se constituyó en el seno del Consejo de Europa una Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad hacia los derechos de las personas, especialmente en relación con su derecho a la intimidad. Como fruto de la Comisión Consultiva surgió la Resolución 509 de la Asamblea del Consejo de Europa sobre los "derechos humanos y nuevos logros científicos y técnicos".[23]

En un momento posterior, surgen diversas leyes nacionales alrededor de Europa. De tal forma que en 1977 era aprobada la Ley

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

[22]Si hacemos un recorrido por los antecedentes de este derecho, tenemos varias referencias en los instrumentos internacionales. El artículo 12 de la *Declaración Universal de los Derechos del Hombre* del 10 de diciembre de 1948 establece el derecho de la persona a no ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias o ataques. El texto íntegro se encuentra disponible en el vínculo siguiente: http://www.un.org/es/documents/udhr/ En el mismo sentido, el artículo 8 del *Convenio para la Protección de los Derechos y las Libertades Fundamentales* del 14 de noviembre de 1950, reconoce el derecho de la persona al respeto de su vida privada y familiar de su domicilio y correspondencia. El texto se encuentra disponible en el vínculo siguiente: http://www.acnur.org/biblioteca/pdf/1249.pdf Por su parte, el artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos* (16 de diciembre de 1966), señala que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Disponible en el vínculo siguiente: http://www.cinu.org.mx/onu/documentos/pidcp.htm En el mismo tenor, la *Convención Americana sobre Derechos Humanos* (22 de noviembre de 1969) en su artículo 11 apartado 2, establece que nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Disponible en su integridad en el vínculo siguiente: http://www.oas.org/Juridico/spanish/tratados/b-32.html

[23]José Luis Piñar Mañas, "El derecho fundamental a la protección de datos personales", *Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos*, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España, 2005, p. 20.

de Protección de Datos de la República Federal Alemana, mucho más ambiciosa que su predecesora del *Land de Hesse*. En 1978 corresponde el turno a Francia mediante la publicación de la Ley de Informática, Ficheros y Libertades, aún vigente. Otros países entre los que se emitió regulación en la materia son Dinamarca con las leyes sobre ficheros públicos y privados (1978), Austria con la Ley de Protección de Datos (1978) y Luxemburgo con la Ley sobre la utilización de datos en tratamientos informáticos (1979).[24]

Hacia la década de los años ochenta –cuando comienzan a utilizarse las primeras computadoras personales o PC´s surgen los instrumentos normativos en los que se plasma un catálogo de derechos de los ciudadanos para hacer efectiva la protección de sus datos, así como las medidas de seguridad a observar por parte de los responsables de los ficheros. Es en esta década cuando desde el Consejo de Europa se dio un respaldo definitivo a la protección de la intimidad frente a la potencial agresividad de las tecnologías, siendo decisivo para ello la promulgación del Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal –en adelante, el Convenio 108–.[25]

De modo que, existen diversos instrumentos internacionales que dan fundamento al derecho a la protección de datos personales entre los que destacan los que se desarrollan brevemente a continuación.

3.1 Directrices de la Organización para la Cooperación y el Desarrollo Económico

La recomendación de la Organización para la Cooperación y el Desarrollo Económico –OCDE– en la que se contienen las "Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales" –en adelante, directrices de la OCDE-,[26] fue adoptada el 23 de septiembre de 1980, y constituye

[24]*Ibíd.*

[25]*Ibíd*., pp. 20-21.

[26]El texto completo se encuentra disponible en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

el primer instrumento en el ámbito supranacional que analiza a profundidad el derecho a la protección de datos de carácter personal.[27]

Estas Directrices se emiten partiendo de una realidad innegable que la OCDE vislumbró y que se traduce en tres problemáticas centrales, a saber:

> - El uso de la tecnología para el tratamiento de datos personales, las posibilidades bastantemente extendidas de almacenamiento, contrastación, vinculación, selección y acceso a los mismo que en combinación con la informática y la tecnología de telecomunicaciones, pueden poner los datos personales simultáneamente a disposición de miles de usuarios en lugares geográficamente dispersos y la creación de redes complejas de datos nacionales e internacionales.
>
> - El peligro que representa las disparidades en las legislaciones nacionales tendentes a conciliar la protección de la información de carácter personal con la transmisión de enormes cantidades de datos a través de las fronteras nacionales, a fin de impedir vulneraciones a los derechos fundamentales de los titulares de esa información como el almacenamiento ilícito de datos personales o el abuso o la revelación no autorizada de los mismos.
>
> - La diversidad en las legislaciones nacionales que trae como consecuencia restricciones a la circulación u obstáculos a la libre circulación transfronteriza de los datos personales, ocasionando graves trastornos en importantes sectores de la economía.

Su adopción se fundamenta en la constatación por parte del Consejo de la OCDE de la inexistencia de uniformidad en la regulación de esta materia en los distintos Estados miembros, lo que dificultaba el flujo de los datos personales entre los mismos.[28]

Las directrices de la OCDE se componen de 5 secciones fundamentales. En la primera parte, se establecen las definiciones

[27] Agustín Puente Escobar, "Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal", *Protección de datos de carácter personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos*, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España, 2005, p. 51.

[28] *Ibíd*.

aplicables, la parte segunda señala los principios básicos relativos al tratamiento de los datos personales. Por su parte, la tercera sección está dedicada a las transferencias internacionales de datos y la cuarta trata, en términos generales, sobre los medios de implantación de los principios básicos expuestos en las partes anteriores. Finalmente, la quinta tiene que ver con cuestiones de asistencia mutua entre los países miembros.

De manera específica, el Capítulo II de dichas directrices señala los siguientes principios básicos en materia de protección de datos personales:

> Principio de limitación de la recogida
>
> 7. Debería haber límites en la recogida de datos personales y tales datos deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.
>
> Principio de calidad de los datos
>
> 8. Los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.
>
> Principio de especificación de la finalidad
>
> 9. Los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.
>
> Principio de limitación de uso
>
> 10. Los datos personales no deberían revelarse, hacerse disponibles o utilizarse de otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo:
>
> a. con el consentimiento del sujeto de los datos, o
>
> b. por imperativo legal.
>
> Principio de salvaguardas de seguridad
>
> 11. Los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de

los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.

Principio de apertura

12. Debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.

Principio de participación individual

13. La persona debería tener derecho a:

a. recabar, del controlador de los datos o de otro modo, confirmación de si el controlador tiene o no tiene datos correspondientes a la misma;

b. hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible;

c. que se le den los motivos para ello, en virtud de los subapartados a. y b., si su solicitud fuere denegada y ella pueda impugnar tal denegación, y

d. impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.

Principio de responsabilidad

14. El controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

En resumen, la OCDE con la emisión de estas Directrices intenta equilibrar dos valores básicos fundamentales, a saber: la protección de los datos personales y la libre circulación de estos mismos a nivel internacional.

3.2 Convenio Número 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal

El Convenio 108 es creado con el propósito de garantizar a los ciudadanos de los Estados contratantes, el respeto de sus derechos y libertades.[29] Entró en vigor el 1 de octubre de 1985, en particular para proteger el derecho a la vida privada frente a los tratamientos de datos personales, conciliando el respeto a ese derecho y la libre circulación de la información entre los Estados.

De esta forma el Convenio 108 constituye el primer instrumento de carácter vinculante para los Estados en el que se plasman los principios de la protección de los datos de carácter personal.

En términos del artículo 1, el objeto y fin del Convenio 108 es garantizar, en el territorio de cada Estado Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

En cuanto a su ámbito de aplicación, el Convenio 108 se aplica, en general a los tratamientos automatizados de datos de personas físicas, sin perjuicio de lo cual los Estados miembros podrán aplicar el Convenio a los datos de personas jurídicas y a los tratamientos manuales de datos, aunque tal circunstancia no se imponga obligatoriamente en el Convenio.

El artículo 5 establece los principios rectores que trazan el tratamiento automatizado de los datos de carácter personal:

- Tratamiento leal y legítimo.

- Principio de finalidad: los datos personales deben ser tratados únicamente para finalidades determinadas y legítimas y no utilizados de una forma incompatible con dichas finalidades.

[29]Disponible en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf Es importante mencionar que el convenio atraviesa por una revisión a efecto de modernizar su contenido y alcance derivado de la evolución tecnológica.

- Principio de proporcionalidad: los datos deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado.

- Principio de calidad: los datos personales deben ser exactos (puestos al día).

- Conservación de datos: la información de carácter personal debe ser conservada de tal forma que permita la identificación de los titulares durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Es importante mencionar que la firma del Convenio 108 no proporcionó la suficiente protección homogénea en materia de protección de datos que se había esperado. Esto se debió esencialmente a la naturaleza del Convenio, en virtud de que el mismo, a pesar de tener una naturaleza vinculante, establecía únicamente unos principios mínimos, permitiendo que, posteriormente, fueran los Estados firmantes los que los desarrollaran. Por este motivo se ha mantenido de forma unánime que el punto más débil del Convenio 108 fue, y sigue siendo, su aplicación. Es decir, se deja que sean los Estados miembros los que apliquen y desarrollen los principios contenidos en el Convenio y, de la misma forma, se les da libertad para aplicar las excepciones a los mismos.[30]

3.3 Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas

La Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas del 14 de diciembre de 1990,[31] contiene fundamentalmente una lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial. Se mencionan, entre otros, los principios de licitud, exactitud, finalidad, acceso y no discriminación.

[30]Mónica Arenas Ramiro, *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, España, 2006, p. 156.

[31]El texto completo se encuentra disponible en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

Los principios consignados en la Resolución 45/95 deben ser aplicables a todos los archivos informatizados públicos y privados, pudiendo extenderse dicha aplicación a los archivos manuales y a las personas jurídicas que contengan alguna información relativa a personas físicas, mediante la expedición de disposiciones especiales. [32]

Ahora bien, la lista básica de principios reconocidos por esta Resolución son:

- Principio de legalidad y lealtad: la información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales.

- Principio de exactitud: las personas responsables de la compilación de archivos o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados y garantizar que los mismos se mantengan de la forma más completa posible.

- Principio de especificación de la finalidad: la finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada.

- Principio de acceso de la persona interesada: cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.

- Principio de no discriminación: sin perjuicio de los casos susceptibles de excepción, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

[32]Consúltese el Artículo 10 de dicho documento. *Ibíd.*

- Principio de seguridad: deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, pérdida o destrucción accidental, como peligros humanos que se traducen en acceso no autorizado, uso fraudulento de los datos o la contaminación mediante virus informáticos.

- Autoridad garante: el derecho de cada país debe designar a una autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios establecidos. Esta autoridad deber ser imparcial, independiente frente a las personas o agencias responsables de procesar y establecer los datos y con competencia técnica.

- Transferencias internacionales: debe existir un flujo libre de datos personales entre los Estados en el cual se establezcan garantías suficientes de protección a la vida privada.

3.4 Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos

La Directiva 95/46, fue aprobada con un doble objetivo: por un lado garantizar el derecho a la vida privada reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos, en particular por lo que respecta al tratamiento de datos personales, ampliando los principios ya recogidos en otras normas internacionales y otorgando un mayor nivel de protección dentro de la Comunidad, sin disminuir el ya existente; y, por otro lado, impedir la restricción de la libre circulación de los datos personales en todos los Estados miembros de la Unión Europea.[33]

El proyecto de Directiva 95/46, se inspira esencialmente en la doctrina constitucional alemana y en la ley francesa de 1978. Sin embargo, los trabajos se paralizaron, dado que diversos estados consideraron que no era posible la aprobación por parte de las instituciones comunitarias de una norma reguladora de un derecho fundamental de los ciudadanos, al no tener tal hecho cabida en las normas rectoras del Derecho Comunitario vigentes en ese momento.[34]

[33]Mónica Arenas Ramiro, *Op. cit.*, pp. 277-278.

[34]Agustín Puente Escobar, *Op. cit.*, p. 43.

A partir de ese momento, los trabajos se centraron en la necesidad de adoptar un texto de Directiva 95/46 referido a la adopción de un marco comunitario que garantice la libre circulación de los datos de carácter personal, no pudiendo los Estados miembros invocar el derecho a la protección de datos como justificación para impedir dicha libre circulación.[35] En ese sentido, la directiva resultaba indispensable para la consecución de mercado único.

Finalmente, la Directiva 95/46 fue aprobada el 24 de octubre de 1995.[36] Con base en esta directiva, los Estados miembros de la Unión Europea han transpuesto en sus normas nacionales los principios que regulan un derecho fundamental sin entorpecer el flujo de información.

Citando a Puente Escobar,[37] las innovaciones introducidas por la Directiva 95/46/CE pueden esquematizarse de la siguiente manera:

- La ampliación del ámbito de aplicación.

- La regulación del encargado del tratamiento.

- El desarrollo de los principios de calidad.

- El "interés legítimo" como legitimador del tratamiento.

- La cláusula sobre la libertad de expresión.

- El reconocimiento del derecho de oposición.

- El reconocimiento de los derechos relacionados con las decisiones individuales automatizadas.

- El desarrollo de sistemas de autorregulación sectorial.

- El régimen sistemático de las transferencias internacionales de datos.

[35]*Ibíd*.

[36]Actualmente, la Directiva 95/46 está en proceso de revisión para su modernización debido al avance tecnológico –como el cómputo en la nube– que obligan a modificar conceptos tradicionales como el de tratamiento de datos, entre otros.

[37]*Ibíd*.

- El reforzamiento de las funciones de las autoridades de protección de datos.

- La creación del Grupo del Artículo 29.

En materia de principios, la Directiva 95/46/CE dispone en el artículo 6 lo que a continuación se indica:

Artículo 6.-

…

1. Los Estados miembros dispondrán que los datos personales sean:

a. tratados de manera leal y lícita;

b. recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas;

c. adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;

d. exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados;

e. conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente.

Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

…

3.5 Carta de Derechos Fundamentales de la Unión Europea

La Carta de Derechos Fundamentales de la Unión Europea,[38] fue aprobada el 7 de diciembre de 2000 por la Cumbre de Jefes de Estado y de Gobierno celebrada en la ciudad de Niza, Francia. Reconoce entre otras cuestiones, el derecho a la protección de datos con el carácter de fundamental en su artículo 8 al establecer que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, sin hacer mención a la intimidad o a la vida privada. También el artículo 8 señala que "el respeto de estas normas quedará sujeto al control de una autoridad independiente".

De esta forma, a partir de su aprobación la protección de los datos de carácter personal se configura como un derecho fundamental y autónomo del derecho a la intimidad y a la privacidad de las personas. Cabe precisar a este respecto, que en su artículo 7 aborda los derechos de manera separada, recoge el derecho a la vida privada y familiar.[39]

Ahora bien, cabe mencionar que paralelamente ha habido un rico desarrollo jurisprudencial que por razones de espacio no se

[38]Disponible en el vínculo siguiente: https://www.agpd.es/portalweb/canaldocumentacion/legislacion/union_europea/common/pdfs/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf

[39]A este respecto, cabe señalar que en México, la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* es la primera pieza legislativa que reconoce por primera vez la protección de los datos personales en este territorio. Este instrumento normativo se limita a las bases de datos del sector público a nivel federal, en virtud de que es, a la vez, una ley de acceso a la información y una ley de protección de datos personales.

En la actualidad en México se reconoce a nivel constitucional el derecho a la protección de datos personales como una garantía fundamental en el artículo 16, al señalar lo siguiente:

Artículo 16.

…

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Para mayor información, sobre el texto constitucional reformado consúltese el siguiente vínculo: http://www.diputados.gob.mx/LeyesBiblio/

desarrollará exhaustivamente, sin embargo, es importante señalar en concreto el caso particular del Tribunal Constitucional Español, el cual arrojó luz sobre el contenido y alcances del derecho a la protección de datos personales en su sentencia 292 del 30 de noviembre de 2000,[40] por la cual definió los contornos de este nuevo derecho al establecer a la letra lo siguiente:

> 7…
>
> [E]l contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular.

Sin afán de exhaustividad, los instrumentos internacionales aquí referidos dan forma y contenido al derecho de la protección de datos, al tiempo de sentar las bases para su reconocimiento y difusión en otras regiones del mundo.

4. La protección de datos personales de niñas, niños y adolescentes

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

[40]Disponible en el sitio oficial del Tribunal Constitucional de España en el vínculo: http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467

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.

Empero, no existe un modelo único de regulación a este respecto. Por un lado, contamos con el modelo europeo, que podría denominarse como universal al ser comprehensivo para la protección de los datos personales (ya que prevé los principios, derechos, procedimientos y autoridad independiente) el cual ha sido adoptado con matices e innovaciones importantes por países como Canadá. Por otra parte, existen modelos sectoriales en los que conviven algunas regulaciones específicas y mecanismos de autorregulación. En este último grupo podríamos ubicar a los Estados Unidos de América.[41] El caso mexicano es más bien un modelo de regulación híbrida, ya que si bien contiene los principios, derechos y procedimientos en materia de protección de datos ante una autoridad independiente; también recoge mecanismos de autorregulación y no exige registros de bases de datos ni autorizaciones de la autoridad para las transferencias internacionales.

Es importante mencionar que en el ámbito europeo, así como en Canadá, las autoridades en materia de protección de datos han promovido intensamente el derecho a la protección de datos de menores a través de campañas de sensibilización dirigidas a padres y educadores, folletos informativos, creación de sitios en Internet de autoayuda, concursos, entre otros mecanismos para fomentar el conocimiento y alcances de este derecho fundamental.

Hay que recordar que la definición de dato personal adoptada de manera *quasi* generalizada en el ámbito internacional, señala que se trata de información relativa o concerniente a una persona física, identificada o identificable. En ese sentido, el ámbito de protección es hacia la persona en relación con el tratamiento que se

[41]Al respecto, cabe precisar que en materia de protección de datos en México, hasta antes de la entrada en vigor de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* se había optado por un modelo sectorial al existir disposiciones para la protección de datos de ficheros crediticios y de solvencia patrimonial; sobre confidencialidad de datos de salud; sobre la existencia de listas de no llame para servicios financieros y de prospección comercial, entre otras.

Asimismo, el tratamiento de las bases de datos en posesión del sector público, en el ámbito federal, se regula a través de la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.*

dé a su información, la cual se puede encontrar en posesión de los gobiernos o de los particulares.

Por lo anterior, puede decirse válidamente que las niñas, niños y adolescentes gozan, en tanto que *son* personas, del derecho a la protección de sus datos personales, el cual se traduce en la debida observancia de una serie de principios y derechos, tutelados a través de un procedimiento, ante una autoridad independiente como se verá en el siguiente apartado.

La falta de dicha observancia ha traído consigo no solo la violación del derecho de protección de datos personales, sino implicaciones en el desarrollo social, psicológico y emocional de muchos de los menores. Existen innumerables casos ilustrativos de las consecuencias de dicha carencia, que por razones de espacio no podemos exponer, sin embargo, se describen cuatro casos ilustrativos y recientes al final del documento para mayor referencia.

5. La propuesta del *Memorándum de Montevideo* sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes

Ahora toca el turno de explicar las distintas propuestas del Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, mejor conocido como *Memorándum de Montevideo* –en adelante, el Memorándum -, para lograr la efectiva protección de los datos personales de las niñas, niños y adolescentes, en éste ámbito.

En este sentido, México sentó las condiciones para adoptar un modelo universal y comprehensivo de protección de datos. Confirma lo anterior, las reformas constitucionales a los artículos 16 y 73 constitucional, por las cuales se dota de contenido al derecho a la protección de datos personales y facultades al Congreso Federal para legislar en materia de protección de datos personales en posesión del sector privado.

Para dar cumplimiento a este mandato constitucional el 5 de julio de 2010 se publicó en el Diario Oficial de la Federación la *Ley Federal de Protección de Datos Personales en posesión de los Particulares*, entrando en vigor al día siguiente.

Hasta este punto, cabe destacar que el 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".[42]

Ahora bien, el objeto de la elaboración del Memorándum nace del reconocimiento de los riesgos a los que están sujetos los menores al momento de navegar en Internet. Los niños, niñas y adolescentes conciben el espacio virtual como un espacio privado, con la posibilidad de actuar y expresarse libremente sin estar plenamente conscientes sobre el control de su información y las implicaciones existentes. Esto genera "bienestar físico y psicológico, así como espiritual" como se ha demostrado desde el ámbito de la psicología.[43]

Más claro, el derecho a la protección de datos personales y la privacidad de los menores se traduce en la no injerencia, el respeto a su dignidad e identidad como personas. Si bien es cierto, el avance tecnológico y la vinculación de los menores con las nuevas tecnologías representa un elemento del proceso evolutivo de la sociedad, también es cierto que este nuevo espacio debe ser regulado para proteger los derechos de la niñez en todos sus ámbitos. Mismos, que al no ser garantizados tendrían implicaciones en su desarrollo y en la estigmatización social consiguiente.[44]

[42]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.europea.eu/justice_home/fsj/privacy/index_en.htm

[43]S.M. Jourard, "Some Psychological aspects of Privacy", *Law and Contemporary Problems*, Duke University School of Law, no. 31, 1966, p. 307. Además, P.B. Newell, "A System of Model Privacy", *Journal of Environmental Psychology*, Publisher Academic Press, no. 14, U.K., 1994, p. 65.

[44]Milton 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. A este respecto, cabe mencionar que algunas de las consecuencias de la falta de garantías al derecho de protección de los datos personales de los menores podría verse reflejado en el futuro en ámbitos como el empleo. Ilustrando este punto, el periódico mexicano El Universal el 28 de septiembre de 2009, señala que cerca de 8.5 millones de internautas en América Latina han ingresado su perfil en alguna red social, lo que en ocasiones ayuda a reclutadores a complementar la información. La empresa de clasificados de

Por lo que hace a las redes sociales, el uso que de ellas hacen los niños, niñas y adolescentes y los abusos a los que podrían ser sujetos, a continuación se abordan las secciones medulares en referencia a la protección de datos y la responsabilidad del Estado y de la Industria. Si bien, el Memorándum aborda diferentes aristas de la problemática, en las secciones sucesivas se analizan respecto de la aplicación al derecho fundamental de la protección de datos personales y las implicaciones en la vida presente y futuro de los menores.[45]

5.1 Recomendaciones para los Estados sobre el marco legal

A este respecto, cabe destacar el numeral 6 denominado "Recomendaciones para los Estados sobre el marco legal" que a la letra establece lo siguiente:

> 6. La protección de los datos personales requiere del desarrollo de una normativa nacional, aplicable al sector público y privado, que contenga los derechos y principios básicos, reconocidos internacionalmente, y los mecanismos para la aplicación efectiva de la misma. Los Estados deberán tomar en especial consideración, en la creación y en el desarrollo de dichas normativas, a las niñas, niños y adolescentes.

La mención anterior tiene varias implicaciones relativas a la protección de los datos personales de los menores. La primera es que

empleo *online* en Latinoamérica, Bumeran.com, expone que 42% de los reclutadores busca información extra de los candidatos a algún puesto a través de Internet. El principal buscador al que los contratantes recurren es *Google* con 35%, seguido de redes sociales como *Facebook* con 25%, *LinkedIn* con 15% y *MySpace* con 5%.

Precisa que la encuesta se llevó a cabo del 1 al 15 de septiembre de 2009 con directores de recursos humanos de Argentina, México, Chile, Colombia y Venezuela. De acuerdo con los resultados, 26% de los reclutadores ayuda a los candidatos a avanzar al siguiente paso debido a la información digital que encuentran en Internet. Si bien 70% de la decisión para contratar a alguien depende de la entrevista, también buscan información de forma externa por lo que en ocasiones 27% de los candidatos pierde la oportunidad de ser contratados, en la mayoría de las veces, por falsedad de información. A mayor abundamiento, consúltese el vínculo siguiente: http://www.eluniversal.com.mx/articulos/55885.html

[45]Existen innumerables casos de los riesgos potenciales a los que se encuentran sujetos los menores al navegar por internet e interactuar en redes sociales. De forma ilustrativa se exponen cuatro casos al final del presente texto a manera de anexo, donde es posible apreciar los impactos físicos, psíquicos, emocionales y jurídicos que la invasión a la privacidad de menores y la vulneración del derecho a la protección de datos personales puede ocasionar.

los Estados que utilicen como principios orientadores el Memorándum a la hora de legislar en materia de protección de datos personales deberán contemplar, entre otros los aspectos que se señalan a continuación.

En principio, el ámbito de aplicación de la norma debiera ser para entes públicos –el Estado en todos sus niveles de gobierno– así como para entes privados, esto es, toda persona física o moral que lleve a cabo el tratamiento de datos personales. La emisión de una ley de protección de datos brindaría la garantía a toda persona –incluidos los menores de edad– de que su información será manejada conforme a lo que establezca esta ley, por lo que si bien, el Memorándum se enfoca a la protección de menores de edad, se recomienda la expedición de una norma de aplicación general, dado que los principios y derechos que se desarrollan en los siguientes párrafos, también son transversalmente aplicables sin distingo de edad, aunque explicaremos las variaciones en su ejercicio al caso concreto.

Una novedad del Memorándum es la recomendación al legislador de tomar en cuenta en el proceso legislativo y de diseño de la norma, la opinión de las niñas, niños y adolescentes, sobre todo, en aquellas disposiciones particulares que se refieran a la forma en que debe llevarse a cabo el tratamiento de su información en Internet, de modo que ellos puedan aportar su opinión.

5.1.1 Los principios de protección de datos

En cuanto a los principios de protección de datos, existe un consenso más o menos generalizado a nivel internacional en reconocer los siguientes:

- Consentimiento;
- Información;
- Finalidad;
- Proporcionalidad;
- Calidad, y
- Seguridad.

Es importante mencionar que como premisa principal el proveedor de toda red social digital debiera comprometerse al tratamiento leal de los datos que no se traduce en otra cosa sino en el hecho de efectuarlo con estricto apego y respeto a los derechos del titular de la información, y sin que medie fraude o engaño.

Por ello, el consentimiento es el principio rector del derecho a la protección de datos personales dado que se trata del poder de disposición del titular de la información para decidir quién, cómo, cuándo y para qué utiliza sus datos, pudiendo oponerse a dicha utilización.

Aquí hay un punto importante a dilucidar y es el tema de la edad ya que no existe consenso acerca de a partir de qué edad se considera que un niño es maduro para poder ejercer su consentimiento y por tanto, manifestar su voluntad para otorgar su información personal sin necesidad de consentimiento otorgado por los padres o tutores. Dicha cuestión dependerá de la legislación que adopte cada país y de conformidad a ello, se establecerían las modalidades para expresar el consentimiento.[46]

[46]En el caso español el Real Decreto 1720/2007 de 21 de diciembre de 2007 por el que se expide el Reglamento de la Ley Orgánica de Protección de Datos, señala en su artículo 13 lo siguiente:

"Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningun caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores o representantes legales".

Ahora bien, otra complejidad se presenta a la hora de comprobar por parte de la industria, que realmente se obtuvo el consentimiento de un menor con la edad establecida por ley. Ello implica el desarrollo de mecanismos para conocer de manera fehaciente, la madurez del titular del dato.

En cuanto al principio de información, este se traduce en la obligación del proveedor de una red social digital de dar a conocer los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, el nombre del responsable de su tratamiento y los medios que ofrecen al titular de los datos para ejercer los derechos de acceso, rectificación, cancelación y oposición (ARCO). También se conoce como el principio de la transparencia en el tratamiento de la información ya que se está utilizando información ajena y por tanto, debe ventilarse de qué manera se hará uso de la misma y bajo qué condiciones podrá el titular de los datos, ejercer los derechos a que se refiere el próximo apartado.

Un aviso de privacidad completo se traduce en la política de privacidad del responsable del tratamiento. En este punto es importante mencionar la complejidad de adjuntar una leyenda clara que no entorpezca la prestación de un servicio, piénsese en las aplicaciones en celulares o teléfonos móviles.

Veamos ahora el principio de finalidad que consiste en que los datos se recaban para cierto objeto concreto y conocido de antemano. Si la finalidad cambia, es necesario obtener el consentimiento del titular para poder utilizar los datos para nuevos objetivos.

Por su parte, el principio de proporcionalidad se traduce en que al tener el tratamiento una finalidad concreta, los datos que se recaben deberán ser directamente proporcionales, pertinentes y no excesivos en relación con dicho fin. Asimismo, debe darse un tratamiento mínimo a la información, ya que en la medida que se obtenga más datos, podría rebasarse el fin primario. A este principio también se le conoce como principio de minimización del tratamiento de los datos.

En lo que respecta al principio de calidad de los datos, éste consiste en mantenerlos actualizados y puestos al día de modo que reflejen verazmente la información acerca de una persona. Un dato inexacto es un dato falso y no rectificarlo podría acarrear consecuencias nefastas.

Finalmente, los datos deben estar seguros, es decir, íntegros y accesibles sólo para aquellos que estén autorizados para ello, como se verá más adelante.

5.1.2 Los derechos de las niñas, niños y adolescentes en materia de protección de datos

Por lo que respecta a los derechos del titular de los datos, también hay coincidencia internacional en reconocer los siguientes:

- Acceso;

- Rectificación;

- Cancelación, y

- Oposición.

Para saber cómo se despliegan los derechos de las niñas, niños y adolescentes a la protección de sus datos personales, el Memorándum en el apartado denominado "Recomendaciones para los Estados sobre el marco legal" en su numeral 8 establece lo siguiente:

> 8. Los Estados deben legislar el derecho que tienen las niñas, niños y adolescentes directamente o por medio de sus representantes legales, a solicitar el acceso a la información que sobre sí mismos se encuentra en bases de datos tanto públicas como privadas, a la rectificación o cancelación de dicha información cuando resulte procedente, así como a la oposición a su uso para cualquier fin.

De acuerdo con dicho numeral, queda claro que los menores de edad podrían solicitar acceso a la información personal que de ellos se conserve, manipule y transmita en las redes sociales. Este derecho se relaciona directamente con el principio de información, ya que solo mediante un aviso de privacidad en el que se establezca la persona responsable del tratamiento de los datos, así como los derechos que tiene el titular de la información, los menores de edad podrán conocer qué información se detenta de ellos.

También deben poder solicitar la rectificación de datos erróneos o desactualizados para su puesta al día. Este derecho se relaciona directamente con el principio de calidad a que se hizo referencia en el apartado anterior. Finalmente, podría pedirse la cancelación

del dato que trae como consecuencia la supresión o eliminación de dicha información. Cabe mencionar que en este punto es importante establecer mecanismos efectivos de supresión total de la información, porque en ocasiones se solicita eliminar una invitación a formar parte de una red social y esta sigue apareciendo *ad infinitum*, sin que sea respetada la voluntad del interesado o titular del dato.

El derecho de oposición también debe poder ejercitarse cuando los datos se hayan obtenido sin el consentimiento de los menores de edad (por encontrarse en fuentes de acceso público por ejemplo) y en este caso, la consecuencia sería la cancelación del dato.

5.1.3 El procedimiento de tutela y autoridad independiente

Ahora me referiré a los alcances de la mención que contiene el Memorándum a los "mecanismos para la aplicación efectiva de la norma". Esta cuestión se refiere a la necesidad de que la norma prevea un procedimiento de tutela de derechos efectivo, expedito y gratuito ante una autoridad independiente.

La autoridad no necesariamente tendría que ser –aunque idealmente sí- una autoridad especializada en protección de datos personales, bien podrían llevar a cabo dicha tarea las defensorías del pueblo o comisiones de derechos humanos, las procuradurías o los jueces. Por ello, resulta relevante que el procedimiento sea expedito y claro para no hacer nugatorio el derecho.

5.2 Recomendaciones para la Industria en materia de protección de datos

En ese sentido, el Memorándum establece que las empresas que proveen los servicios de acceso a Internet, desarrollan las aplicaciones o las redes sociales digitales, deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada —en particular de niñas, niños y adolescentes—, a cooperar con los sistemas de justicia nacionales, desarrollar campañas de prevención y desarrollo de capacidades, entre otros instrumentos mediante compromisos o códigos de conducta, que deben incluir:

> 19. No permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la

información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento.

También se señala que en el caso de niñas y niños se deberá considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara.

Dado que en varios países ya existe la obligación para la industria de establecer controles para limitar la información que las niñas y niños proporcionan en Internet, el Memorándum al señalar de manera contundente que la industria deberá considerar la prohibición del tratamiento de datos de niñas y niños, lo que se busca es que limitar la recolección y almacenamiento de información *solo al caso de los adolescentes.*[47]

[47]El caso español es ilustrativo a este respecto. En 2009 la Agencia Española de Protección de Datos -en adelante, AEPD- publicó una nota informativa en la cual destaca la alta desconfianza de los ciudadanos españoles en la seguridad de sus datos en Internet. Al respecto, para un 56.6 % de los ciudadanos españoles encuestados, Internet ofrece una seguridad de sus datos baja o muy baja. El 73.9 % de los ciudadanos se muestra preocupado por la protección de su privacidad, lo que revela una creciente concienciación de éstos acerca del valor de su información personal.

Por su parte, el Centro de Investigaciones Sociológicas (CIS) publicó su barómetro correspondiente al mes de septiembre de 2009, el cual se refleja una creciente preocupación de los españoles por la protección de datos y el uso de su información personal. El barómetro destaca que este asunto preocupa bastante al 43.5% de los españoles y mucho al 30.6% de los encuestados, situándose por delante de asuntos como el avance de la ciencia y la tecnología, el desarrollo de la comunicación a través de Internet y la piratería. En relación a la confianza de los españoles en torno al grado de seguridad de sus datos, el barómetro arroja que Internet es el lugar en que los usuarios creen que la seguridad y privacidad de los datos es más deficiente, un 56.6% de los ciudadanos destacan que Internet les ofrece la seguridad baja o muy baja, seguido de compañías de teléfono, agua, gas, comercios y bancos.

Además, si bien los ciudadanos destacan que Internet facilita que la gente se mantenga informada y la comunicación entre las personas, más del 70% cree que su uso favorece la intromisión en la vida privada de las personas. Asimismo, son los servicios en los que existe un mayor potencial de difusión de información personal propia o de terceros, como las redes sociales -un 48% asegura que su seguridad es baja o muy baja- y los servicio de mensajería y chat los que generan más desconfianza.

De hecho según se destaca, publicar fotos o videos propios o de familiares o amigos en Internet ofrece para el 76.7% de los españoles poca o ninguna seguridad. Asimismo, la encuesta revela que más del 65% de ciudadanos admite que nunca o raramente lee las políticas de privacidad de los sitios que visita.

Lo anterior tiene una lógica subyacente y es el hecho de que a partir de cierta edad, el ser humano comienza a ser consciente de su voluntad y de los efectos de sus actos u omisiones. En la infancia, la inocencia de las niñas y niños los lleva a intercambiar toda la información que le soliciten acerca de sí mismos, así como de sus padres, hermanos y amigos, a cambio de –por ejemplo– conseguir puntos para ver a sus mascotas virtuales favoritas. Aquí tenemos una clara tensión entre el modelo de negocio de juegos para menores en redes sociales y los derechos de la niñez.

Conviene aquí recordar que la Convención sobre los derechos de los niños establece que no serán objeto de injerencias por lo que la prohibición al tratamiento de datos de niños no surge en el Memorándum, sino que más bien se retoma de los derechos del niño reconocidos en los instrumentos internacionales. En otras palabras, la actividad que actualmente lleva a cabo la industria al

Para la AEPD, estos datos confirman la urgente necesidad de que los proveedores de servicios mejoren sus políticas informativas y de privacidad e incrementen las garantías que ofrecen a sus usuarios. En esta línea, la AEPD actualmente trabaja activamente con los principales prestadores de servicios de redes sociales con el objeto de que adecuen sus prácticas a la normativa de protección de datos.

Respecto a la relación menores-Internet, la AEPD ha valorado muy positivamente el hecho de que la mayor parte de los ciudadanos, más del 80%, considere necesario que los menores de edad cuenten con controles en el acceso a Internet. El barómetro revela que los ciudadanos apuntan a los padres como responsables para establecer los citados controles en primer lugar, por delante de profesores de escuela o el propio gobierno. Si bien, según destaca la encuesta que entre las familias con hijos menores y que disponen de Internet, la inmensa mayoría -el 80.7%- asegura que ejerce control sobre ellos cuando navegan por la red, principalmente limitando el tiempo o el tipo de páginas web, sólo un 34% ejerce un control real al exigir al menor que esté acompañado.

En relación a esta cuestión, Artemi Rallo, director de la AEPD, ha destacado que la presencia incontrolada de menores en la red es hoy una de las principales preocupaciones de la agencia y ha reclamado que exista un compromiso real y activo tanto de padres, autoridades educativas y proveedores de servicios con la protección de los menores en la red. Asimismo, el director ha recordado que existe una obligación legal de los prestadores de servicios de Internet de establecer controles que limiten que los menores de 14 años faciliten datos en Internet, cuyo cumplimiento es hoy por hoy poco satisfactorio, y que es igualmente necesario que exista un compromiso de las autoridades educativas para que sea incorporado en los planes de estudio la educación de los menores en el uso seguro de las nuevas tecnología.

Para mayor información consúltese el vínculo: https://www.agpd.es/portalweb/revista_prensa/revista_prensa/2009/notas_prensa/common/oct/151009_nota_prensa_barometro_cis.pdf

recabar información que los propios niños proporcionan en redes sociales, tiene claros vicios del consentimiento, por lo que en algunos casos podría resultar una actividad ilícita.

Ahora bien, en el caso de los adolescentes, de acuerdo con las edades que cada país determine, éstos podrían proporcionar algunos de sus datos, siempre y cuando puedan conocer de manera clara las reglas del juego que bien podría denominarse "intercambio de privacidad a cambio de diversión" como veremos más adelante.

Otras recomendaciones a la industria en materia de protección de datos, establecen lo siguiente:

> 20. Proteger la vida privada debería ser la característica general y por defecto en todas las redes sociales digitales, bases de datos y sistemas de comunicación, entre otros. Los cambios en el grado de privacidad de su perfil de usuario que se quieran realizar deben ser sencillos y sin costo alguno.
>
> 21. Las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes.
>
> Se deberá proveer información sobre los propósitos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a terceros. De igual modo se deberá indicar la persona o personas responsables del tratamiento de la información.
>
> …

Esta mención es importante, ya que dicha recomendación se traduce en la obligación de la industria de proveer los llamados avisos de privacidad para dar cumplimiento al principio de información antes abordado. En ese sentido, el aviso deberá transmitir de forma clara y sencilla las reglas sobre privacidad, los propósitos y finalidades para los cuales serán utilizados los datos y/o transmitidos a terceros, así como el nombre del responsable de su tratamiento, dado que si no se le puede identificar claramente, tampoco podrían ejercitarse los derechos de acceso, rectificación, cancelación u oposición. A mayor abundamiento, el Memorándum establece lo siguiente:

> …
>
> Se debe igualmente ofrecer un enlace hacia los "parámetros de privacidad" en el momento de la inscripción, conteniendo una explicación clara sobre el objeto de dichos parámetros.
>
> Debe hacerse accesible igualmente un aviso sobre el hecho de que la red social ha preseleccionado los parámetros, si éste es el caso, y que pueden ser cambiados en todo momento, según las preferencias de las niñas, niños y adolescentes.
>
> Sería deseable igualmente que se cambien los "parámetros por defecto" de los contenidos personales, para que puedan ser únicamente accesibles por los amigos y las redes que el usuario determine.
>
> 22. Toda red social digital debe indicar explícitamente en la parte relativa a la "publicidad" contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.
>
> 23. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital.
>
> Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria.
>
> La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.
>
> 24. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley.
>
> Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su

> cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable. Asimismo se deberá eliminar la información de no usuarios, considerando un límite razonable de conservación cuando han sido invitados a ser parte de las redes. Las redes sociales digitales no deben utilizar la información de no usuarios.
>
> Las dos opciones que permitan desactivar y suprimir las cuentas deben ser totalmente visibles para los usuarios, que deben poder comprender qué supone cada opción en cuanto a la gestión por parte del servicio de los datos contenidos en dichas cuentas.
>
> Se tiene que informar a los usuarios de las obligaciones de privacidad frente a terceros, dicha política debe ser explícita, clara y visible.
>
> 25. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. *La indexación de información de niñas y niños debe estar prohibida en todas sus formas*, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos.
>
> [*énfasis añadido*]

Uno de los aspectos que más han preocupado a las autoridades de protección de datos en el mundo, así como a otros actores importantes, es el hecho de que la información que se "sube" a las redes sociales se indexa a buscadores en Internet. Lo anterior significa que si la gente no está consciente de ello y no cuenta con la información necesaria ni los mecanismos para oponerse a esa acción, toda la información que considera que comparte únicamente con sus "amigos" en la red, también puede ser conocida y copiada por el resto de la gente que pueda tener acceso a buscadores comunes de información. Bastaría entonces con buscar el nombre de una niña, niño o adolescente, para que cualquier persona sin ser su "amigo" pueda saber todo lo que hace y quienes forman parte de su círculo social, además de otra información derivada.

Por ello, en el caso particular de las redes sociales digitales, se ha solicitado por autoridades como la Comisaria Europea para la Sociedad de la Información, que dichas redes garanticen que "al menos" las cuentas de los menores de edad sean "privadas por defecto e inaccesibles" a través de los buscadores de la red. Lo anterior busca la mayor protección de los menores dado que no podrían indexarse

los datos de menores en las herramientas para la búsqueda de información en Internet, impidiendo seguir su rastro.[48]

En lo que respecta al acceso por parte de terceros, el Memorándum en cuestión dispone lo siguiente:

> 26. Toda red social digital debe establecer las medidas necesarias para limitar el acceso por parte de los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros), a los datos personales de los usuarios cuando éstos no sean necesarios ni pertinentes para el funcionamiento de dichas aplicaciones.
>
> La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas únicamente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación.
>
> Es igualmente importante que se tomen las medidas necesarias para evitar toda comunicación de datos personales de aquellos usuarios que no han decidido expresamente por ellos mismos el instalar alguna aplicación.

De nuevo, el hilo se rompe por lo más delgado. Un argumento muy socorrido por la industria es el hecho de que ellos no tienen interés en identificar a las personas, sino únicamente manejar información disociada para que los proveedores puedan hacerles la vida más fácil, ofreciéndoles bienes o servicios *ad hoc* a sus gustos y necesidades. A esta actividad se le denomina 'perfiles basados en comportamiento' o *behavioral targeting*.

[48]De acuerdo con una nota publicada por la revista de derecho informático Alfa-Redi publicada el 19 de octubre de 2009, el *boom* de las redes sociales en Internet ha contribuido al incremento de la desaparición de menores de edad en Lima, muchos de los cuales caen en manos de mafias de trata de personas. En ese año, se reportaron más de 600 adolescentes desaparecidos solo en Lima.

El jefe de la División de Investigación de Desaparecidos de la Policía Nacional, José Luis Langle, declaró al rotativo que las denuncias por desaparición de personas pueden llegar hasta a ocho casos diarios. A mayor abundamiento, consultar los vínculos siguientes: http://www.alfa-redi.org/rdi.shtml, además en: http://www.alfa-redi.org/noticias.shtml?x=11602

Sin embargo, si el proveedor del la red social digital no establece medidas para que terceros desarrolladores de las aplicaciones que se ofrecen, estén limitados en cuanto al acceso a los datos personales de los usuarios, se tiene entonces a un sinnúmero de polizontes que aprovechan estos esquemas abiertos.

Por ello, se recomienda la programación de filtros especiales para que dichos terceros sólo puedan obtener aquella información que el titular ha consentido expresamente "compartir" y no toda aquella que se encuentra en su cuenta. Dicha recomendación se hace explícita en el numeral 29, de la forma siguiente:

> 29. La industria debe establecer medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la integridad, disponibilidad y confidencialidad.

Finalmente, la observancia de los principios y derechos en materia de protección de datos personales no serviría de mucho, si no se prevén las medidas necesarias para asegurar que la información no sea accedida por quien no tiene derecho a ella. De igual manera se recomienda prever medidas para garantizar la integridad de la información.[49] Lo anterior es así dado que el gran archivo que conforma la información de millones de personas, constituye uno de los conglomerados de perfiles más detallados y complejos que pueden existir.

Conclusiones

Como se desprende de la larga marcha que han emprendido los derechos humanos, al tiempo que evolucionó la ciencia y la tecnología surgió un nuevo derecho fundamental a la protección de datos personales y la necesidad de desplegar sus mecanismos de tutela, para la efectiva protección de las niñas, niños y adolescentes.

Es claro que la protección de los datos personales como un derecho fundamental y autónomo, contempla en su amplio espectro la salvaguarda de los menores, por el simple hecho de ser. Sin embargo, la realidad nos demuestra la urgente necesidad de comprometernos en todos los niveles para que no se irrumpa en ese ámbito, por demás delicado. La afectación en la vida presente y adulta de los niños, niñas y adolescentes no solo pone en riesgo su integridad personal sino además su desarrollo en todas las esferas de su crecimiento. De ahí, la urgente necesidad de regular las nuevas tecnologías, que si bien nos acercan cada día más, no vienen exentas de peligros.

El uso casi generalizado de los teléfonos móviles trae consigo grandes retos, ya que no todos los menores tienen acceso a una computadora, sin embargo, todos pueden acceder a las redes sociales desde su teléfono y eso complica el cumplimiento de los principios de protección de datos, como el de información y consentimiento, así como la supervisión de los padres y educadores respecto de los contenidos a los que se accede. Las autoridades de protección de datos comparten esta preocupación.

Si bien los Estados no han adoptado un modelo único para la tutela del derecho a la protección de datos, cuando se trata de proteger a la infancia, las cosas cambian. El ejemplo quizá más palpable sea el hecho de que en los Estados Unidos de América existe una ley para proteger la privacidad de los niños cuando navegan en Internet, sin que exista una ley marco en materia de protección de los datos personales de otros sectores de la población.[50] Es por ello que dado que existe consenso en cuanto a la necesidad de proteger a los menores de edad en general en Internet y más recientemente en redes sociales, es necesario actuar para garantizar una tutela efectiva.

[49]El diario mexicano el Informador.com.mx publicó el 12 de octubre de 2009 que la operadora *T-Mobile*, filial de *Deutsche Telekom* informó a sus clientes en los Estados Unidos que perdió todos los datos personales -contactos, citas, listas de tareas, fotos- de los poseedores de teléfonos celulares modelo *Sidekick* que no estuvieran alojados en los mismos, sino en los servidores del servicio. *Sidekick* es una serie de teléfonos avanzados fabricados por la firma *Danger*, que *T-Mobile* comercializa en exclusiva y que combinan el alojamiento local con diversos servicios de *cloud computing*. En siguientes líneas se lee que, el comunicado de *T-Mobile* insta a sus clientes a no retirar la batería de sus *Sidekick*, no reiniciarlos y evitar que se queden sin batería, con el fin de conservar al menos los datos que contienen. Disponible en el vínculo siguiente: http://www.informador.com.mx/tecnologia/2009/144861/6/filial-de-deutsche-telekom-pierde-datos-personales-de-clientes-estadounidenses.htm

[50]Se refiere a la *Children´s Online Privacy Protection Act* de 1998, disponible en el vínculo siguiente: http://www.ftc.gov/ogc/coppa1.htm

Asimismo, al final del presente texto el lector podrá encontrar un cuadro comparativo con cuatro casos normativos relevantes, incluyendo el antes mencionado, para mayor referencia internacional.

Existe la urgente necesidad de que los Estados comiencen a establecer mecanismos integrales de protección que arranquen con la expedición de normatividad en materia de protección de datos, pero que además de manera sistémica, se contemple la prevención a través del fomento educativo sobre los riesgos que enfrentan y las alternativas con que cuentan las niñas, niños y adolescentes al utilizar redes sociales digitales. Lo anterior necesariamente implicará el involucramiento de los poderes judiciales para que una vez que se han conculcado los derechos de los menores de edad, estos puedan ser resarcidos. Es un deber del Estado y una obligación democrática.

La confianza y la seguridad en la utilización del Internet y, en particular de las redes sociales, son aspectos fundamentales en la construcción de una sociedad mundial de información segura y abierta a todos. Ello urge la inmediata cooperación internacional y de abordar la ciber-seguridad de forma holística, resolviendo cuestiones jurídicas, técnicas, orgánicas y procedimentales.

De igual forma, la protección de la infancia en el ámbito tecnológico necesita de los padres. Las barreras tecnológicas instaladas en algunas páginas de Internet, como filtros o mecanismos de verificación de edad e identidad, no han sido suficientes para garantizar un uso seguro de la red a niños y adolescentes. Es necesaria la combinación de estas medidas técnicas con otros elementos, como la supervisión de los padres, la educación, el refuerzo de la ley y la puesta en marcha de políticas de seguridad entre los proveedores y las páginas que alojan redes sociales. La protección de los datos personales y de la integridad del niño demandan un esfuerzo conjunto.

Así como se establece en la Convención sobre los Derechos del Niño, los Estados deben tomar las medidas apropiadas para garantizar que los niños, las niñas y adolescentes sean protegidos y se garantice su bienestar. La experiencia demuestra que el nivel de responsabilidad y el papel de un gobierno en el establecimiento y la defensa de estándares de protección, como el liderazgo de su nación para proteger los derechos de los niños, determina la naturaleza, la cantidad y la calidad de lo que el país logra hacer por sus niños a través de generaciones.

De ahí que la socialización del Memorándum, contribuye a los esfuerzos de la región encaminados a salvaguardar y proteger a la infancia, ante los cambios tecnológicos y las nuevas formas de vida.

Más aun, coadyuva a la transformación cultural que comprende la construcción de la ciudadanía desde el mismo momento en que empieza la vida, y en la fase más importante de formación del ser humano; la infancia.

La protección de sus datos y vida privada en las redes sociales digitales es un paso más a favor de su desarrollo integral, y una obligación de cada Estado miembro. Imprescindible, por tanto, incluir en la agenda nacional la protección de la niñez en el ámbito de las tecnologías.

Anexo Único.

Casos Ilustrativos

Algunos casos prácticos sobre el uso y abuso de las redes sociales para el acoso y explotación de menores, se expone a continuación:

Caso 1. Una adolescente británica a la cárcel por bullying[51] en Facebook.

[51] El *bullying* es una intimidación y maltrato, de forma repetida y mantenida, casi siempre lejos de los ojos de los adultos, con la intención de humillar y de someter abusivamente a una víctima indefensa, por parte de uno o varios agresores a través de agresiones físicas, verbales o sociales con resultados de victimización psicológica y rechazo grupal.

El acoso se define como "una o varias conductas de hostigamiento y maltrato frecuentes y continuadas en el tiempo donde las agresiones psíquicas adquieren mayor relevancia que las físicas". El *bullying* tiene múltiples modos de manifestación, y por tanto es un concepto muy amplio, que engloba todas las formas de violencia o intimidación. Por su parte, el *cyberbullying* es una manifestación del acoso que se produce mediante plataformas virtuales y herramientas tecnológicas, tales como chats, blogs, fotologs, mensajes de texto, correo electrónico, consolas de juegos, páginas webs, redes sociales, teléfonos móviles y otros medios tecnológicos. Incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

Por lo anterior, para ser considerado *cyberbullying*, tiene que haber menores en ambos extremos del ataque. Si hay algún adulto, estamos ante un caso de ciberacoso. Ahora bien, el anonimato, la no percepción directa e inmediata del daño causado y la adopción de roles imaginarios en el internet convierten al *cyberbullying* en un grave problema. A mayor abundamiento, Véase A. Oñate e Iñaki Piñuel, *Mobbing Escolar*, Ediciones CEAC, Madrid, 2007.

País: Reino Unido de la Gran Bretaña (Worcester, Inglaterra), 24 de agosto de 2009. Disponible en el vínculo: http://www.direct.gov.uk/en/YoungPeople/HealthAndRelationships/Bullying/DG_070501

Exposición de caso.

Una adolescente de 18 años se ha convertido en la primera persona encarcelada en Gran Bretaña por hacer 'bullying' e intimidar a una compañera de instituto a través de una la red social.Keeley Houghton había acosado a Emily Moore durante la etapa en la que acudieron juntas al colegio. Houghton se jactaba en su página de Facebook de que iba a matar a su compañera.

La joven inglesa fue condenada a tres meses de encierro en una institución para delincuentes juveniles, tras declararse culpable de acoso. Houghton también recibió una orden de restricción que impide acercarse a Emily Moore, ya sea por internet o por cualquier otro medio.

Observaciones.

A este respecto, cabe destacar que el gobierno británico ha implementado la campaña *"Laugh at it and you are part of it"*,[52] que pretende generar consciencia sobre el ciberbullying y sus consecuencias sociales.

Caso 2. Viví un infierno, todo por ser buen estudiante.

País: Colombia, 6 de septiembre de 2009. Disponible en: http://www.eltiempo.com/archivo/documento/MAM-3606418

Exposición de caso.

El adolescente, que hoy tiene 13 años, estudiaba en un prestigioso colegio de Bogotá. Ingresó en cuarto de primaria. Sus padres lo matricularon allí porque el plantel donde estudiaba no era bilingüe.

[52] Disponible en el vínculo siguiente: http://yp.direct.gov.uk/cyberbullying/

"Venía de un colegio muy estricto -cuenta él-. Estaba acostumbrado a la disciplina, y muchas cosas que enseñaban, ya las sabía. Me la empezaron a montar de nerdo".

Y por eso, por ser estudioso y respetuoso, un par de compañeros empezaron a hacerle la vida imposible. Además de golpearlo e insultarlo a diario, lo excluían todo el tiempo. Lo dejaban solo a la hora del descanso, no le permitían jugar con ellos.

Todo se complicó cuando las agresiones trascendieron al escenario virtual. En el *Messenger* era costumbre que cada uno de los compañeros de curso pusiera, en su estado, un mensaje insultante hacia él. Hacían concursos de la mejor frase, y él las veía cuando se conectaba.

Todo el tiempo recibía mensajes en su correo electrónico y en su celular. El adolescente, narró: "Empecé a tener pensamientos malos, a perder las ganas de vivir. Quise morirme, no quería ser el rechazado del curso". Tal fue la presión que, según su médico de cabecera, sufrió un bloqueo de la hormona del crecimiento.

Caso 3. *Ciberbullying*: Cuatro adolescentes demandados por crear un perfil falso en *Facebook*.

País: Estados Unidos de América, 29 de septiembre de 2009. Disponible en: http//cyberbullying.us/blog/lori-drew-officially-acquitted.html

Exposición de caso.

Cuatro adolescentes han sido acusados por crear un perfil falso de un compañero en *Facebook*, presentándolo como racista y sexualmente obsceno, y en continua búsqueda de nuevos amigos para expandir su red social. El perfil fue suficientemente creíble para hacerse de 580 amigos. Al respecto, la madre del adolescente ha puesto una demanda en contra de los cuatro adolescentes, acusándolos de difamación y por causar stress emocional severo a su hijo.

Aparentemente, los cuatro estudiantes difamaron el nombre de un compañero, usando fotografías y registrando información real en sus datos de contacto, como su número celular. Asimismo, el grupo también expuso numerosas frases obscenas, racistas y sexuales.

El grupo, en nombre del adolescente, efectuaba comentarios denigrantes en contra de los demás miembros asociados en su página. Lo que resultó en un severo desgaste emocional, implicaciones para sus familiares –al tener que cambiar de club social, transporte escolar, etc.–, gastos económicos, entre otros.

La demanda fue hecha ante la Corte de Illinois y busca además del castigo, compensar los daños.

Caso 4. Mi 'ciberamigo' me chantajeaba. Ingresa en prisión un jóven que acosó desde Cádiz a más de 250 mujeres, muchas de ellas menores, a través de la red.

País: España (Cádiz), 15 de junio de 2009. Disponible en: http://www.elpais.com/articulo/sociedad/ciberamigo/chantajeaelpepisoc/20090615elpepisoc_5/Tes

Exposición de caso.

El detenido en Chipiona (Cádiz) era, en realidad, varón y tenía 24 años pero se había inventado hasta 12 personalidades distintas para ganarse la confianza de sus víctimas de diferentes maneras.

Durante semanas habló con ellas a través de Internet. Se intercambiaron palabras en el chat, mensajes por correo y fotografías en algunas redes sociales como *Facebook*.

Cuando la amistad se consolidaba y reunía material suficiente, él desvelaba su verdadero rostro. El que amenazaba y chantajeaba a las que supuestamente eran sus amigas. Así engañó a 250 personas, la mayoría mujeres y menores. La Policía le detuvo una vez en octubre del año pasado. Pero siguió actuando. A la segunda le han llevado a prisión.

El método usado por este delincuente cibernético se conoce como *grooming*, nacido de la revolución que ha supuesto el auge de programas de mensajería instantánea, chats, redes sociales donde es fácil encontrar amigos pero no siempre con buenas intenciones.

La operación policial que ha acabado con el arresto y encar-

celamiento de este joven se ha hecho pública justo cuando el Ministerio del Interior ha emprendido una campaña para advertir de los riesgos de poner en Internet datos e imágenes privados, sobre todos, de menores. El detenido conocía estas facilidades y dominaba la técnica informática y las fórmulas para obtener de sus víctimas lo que buscaba.

La policía conoció los hechos a través de una denuncia registrada en Madrid. Una joven reveló que alguien al que había conocido en Internet la estaba chantajeando. Ella misma le había entregado, en virtud de la confianza ganada, una foto con una imagen suya desnuda. Ahora su supuesto amigo cibernético le amenazaba con difundirla y humillarla públicamente si no le entregaba semanalmente un vídeo de contenido sexual en el que ella apareciera.

Esa denuncia permitió seguir la pista al acosador. La Brigada de Investigación Tecnológica del Cuerpo Nacional de Policía le localizó en octubre de 2008 en Chipiona y se le intervinieron dos ordenadores portátiles y dos discos duros. Fue detenido pero quedó en libertad.

El material intervenido fue analizado y se constató la existencia de más víctimas. Este descubrimiento abrió una nueva investigación que se ha prolongado todos estos meses y que ha permitido cifrar en 250 las víctimas, la mayoría de ellas mujeres y menores de todo el territorio español, aunque también había extranjeras.

El acosador no se limitó a utilizar la información personal que sus víctimas le habían cedido voluntariamente, sino también usó programas de control remoto para acceder al contenido de cuentas de correo electrónico y los archivos personales de sus ordenadores.

Cuadro. Regulación Internacional en materia de protección de datos de menores de edad: Cuatro casos relevantes.

Para mayor referencia sobre la situación que guarda la regulación internacional en la materia, a continuación se exponen cuatro casos ilustrativos.

ESTADOS UNIDOS (FTC)	ITU (International Telecommunication Union)
Children's Online Privacy Protection Act of 1998[53] Dirigido a padres y tutores legales, operadores de páginas web, mensajes en línea, salas de chat y correos electrónico. Objetivo: regular la información en línea recabada por personas físicas o morales dentro del territorio de los E.E. U.U. que contengan datos de niños menores de 13 años. Ámbito de aplicación: - Menores de 13 años. - Padres y Tutores legales. Observaciones: La información sujeta al ámbito de esta ley, será aquella que contenga los datos que se enlistan a continuación. - Nombre. - Domicilio. - Correo electrónico. - Número telefónico. - Número de seguridad social - Cualquier medio de identificación que permita el contacto físico o en línea con un individuo especifico. - Información del menor o de sus padres recolectada por un sitio web.	**Guidelines on Child Online Protection**[54] Dirigidas a padres de familia, niños y adolescentes, incluyendo aquellos con discapacidades que hacen uso del Internet. Objetivo: resaltar la importancia del Internet como herramienta de comunicación, al tiempo que subraya los peligros para los menores. Establece los fundamentos para una navegación segura. Incluye en además de recomendaciones para la navegación segura en chats, correo electrónico, redes sociales, además, juegos en línea. Ámbito de aplicación: - Menores de 16 años. Recomendaciones destacadas: - Derecho a usar internet de manera segura. - Privacidad en redes sociales. - Precaución en la publicación de información personal en internet. - Precaución en la información engañosa. - Respeto a los derechos de las personas. - Comunicación con mayores sobre actividades en la red. - Uso seguro de equipos y dispositivos. - Ubicación de computadoras en lugares visibles. - Medidas de seguridad en los sistemas y controles parentales. - Reglas para el uso de computadores y teléfonos. - Educación y actualización sobre el uso de nuevas tecnologías de información. - Desarrollo de políticas accesibles y apoyo.

[53]Disponible en el vínculo siguiente: http://www.ftc.gov/ogc/coppa1.htm

[54]Presentadas en la reunión de la Unión Internacional de Telecomunicaciones,

ESPAÑA (AEPD)	UNIÓN EUROPEA (Grupo de Trabajo Artículo 29)
Recomendaciones Derechos de niños y niñas deberes de los padres y madres 2008[55] Dirigidas a padres y niños a fin de garantizar el derecho a la protección de datos personales de los menores y mayores de 14 años. Objetivo: hacer del conocimiento de los padres y de los niños una serie de reglas básicas y sencillas a través de las cuales se puede garantizar, en la medida de lo posible, la confidencialidad de la información personal que los menores publican y comparten en Internet, a través de aplicaciones o herramientas informáticas como páginas web, chats, redes sociales, entre otras. Ámbito de aplicación: - Menores de 14 años. - Padres y tutores legales. Recomendaciones destacadas: - Observancia de la normatividad en colegios y servicios de transporte escolar. - Supervisión de los adultos cuando los menores de 14 años naveguen en la red. - Revisión de las políticas de privacidad de los sitios web. - Seguridad y apoyo a los menores que utilicen juegos en línea y servicios de chat o redes sociales - Respeto a la privacidad de los menores usuarios de entornos de red personalizados. - Educación sobre los beneficios y riesgos de las tecnologías de información.	**Documento de trabajo 1/08 sobre la protección de datos personales de los niños**[56] Dirigido a menores dentro del ambiente escolar. El documento ofrece directrices específicas dirigidas a los colegios, específicamente a profesores y autoridades escolares. Objetivo: establecer los principios generales para la protección de los datos de los niños y de manera particular el tratamiento de esta información que se realiza en los colegios -área crítica específica que recaba un sinnúmero de información de sus alumnos-. Ámbito de aplicación: - Menores de 18 años. Recomendaciones destacadas: - Reconocimiento, representación y protección por parte de Padres y Tutores legales. - Intimidad de los menores. - Adaptación al grado de madurez del niño para consultar su consentimiento. - Derechos: Información, acceso (a partir de los 12 años) y oposición. - Expedientes de alumnos. - No discriminación. - Protección en la comunicación de datos. - Solicitud de consentimiento para publicar resultados escolares confidenciales. - Consideraciones sobre la utilización de datos biométricos para acceso al colegio. - Circuito cerrado de televisión CCTV. - Condiciones de salud. - Sitios web de los colegios. - Consideraciones sobre fotografías y credenciales. - Grabaciones de audio y video con teléfonos celulares. Observaciones: Este documento reconoce como derechos fundamentales del niño: el principio de interés superior por el niño; la protección y cuidado necesario para el bienestar de los niños; el derecho a la intimidad; el derecho de representación; entre otros.

efectuada del 5-9 de Octubre de 2009.Disponible en el vínculo siguiente: http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

[55]Disponible en el vínculo siguiente: https://212.170.242.196/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

[56]Encuentra su fundamento en la Directiva 95/46/CE, y retoma los principios de calidad, buena fe, finalidad, conservación, legitimidad, seguridad.

Disponible en el vínculo siguiente: https://212.170.242.196/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2008/common/menores_es.pdf.

Referencias Bibliográficas

ANAYA MUÑOZ, Alejandro *et.al.* (2005), *Glosario de términos básicos sobre derechos humanos*, Comisión de Derechos Humanos del Distrito Federal, Universidad Iberoamericana Ciudad de México, México.

ARENAS RAMIRO, Mónica (2006), *El derecho fundamental a la protección de datos personales en Europa*, Tirant lo Blanch, Valencia, España.

Derecho Internacional de los Derechos Humanos: Normativa, jurisprudencia y doctrina de los sistemas universal e interamericano (2004), Oficina de Colombia del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Bogotá, Colombia.

CANEY, Simon y Peter JONES (eds.) (2001), *Human Rights and Global Diversity,* Frank Cass Publishers, London.

FRIEDMAN, Milton (1990), *The Republic of choice. Law, Authority and Culture,* Harvard University Press, Cambridge.

JOURARD, S.M. (1966), "Some Psychological aspects of Privacy", *Law and Contemporary* Problems*,* Duke University School of Law, no. 31, Durham, NC.

MURILLO DE LA CUEVA, Pablo y José Luis PIÑAR MAÑAS (2009), *El derecho a la autodeterminación informativa,* Fundación Coloquio Jurídico Europeo, Madrid.

NEWELL, P.B. (1994), "A System of Model Privacy", *Journal of environmental Psychology*, Publisher Academic Press, no. 14., U.K.

PIÑAR MAÑAS, José Luis (2005), "El derecho fundamental a la protección de datos personales", *Protección de* Datos *de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos*, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.

—— (2008), *¿Existe la Privacidad?*, CEU Ediciones, Madrid.

OÑATE, Araceli e Iñaki PIÑUEL (2007), *Mobbing Escolar*, Ediciones CEAC, Madrid.

PUENTE ESCOBAR, Agustín (2005), "Breve descripción de la evolución histórica y del marco normativo internacional de la protección de datos de carácter personal"*, Protección de Datos de Carácter Personal en Iberoamérica: II Encuentro Iberoamericano de Protección de Datos*, La Antigua-Guatemala, 2-6 de junio de 2003, Valencia, España.

PUPAVAC, Vannesa (1998), "The Infantilization of the South and the UN Convention on the Rights of the Child", *Human Rights Law Review*, University of Nottingham, Centre for Human Rights, marzo, Reino Unido.

RODRÍGUEZ PALOP, María Eugenia (2002), *La nueva generación de derechos humanos. Origen y justificación,* Dykinson-Universidad Carlos III de Madrid, Madrid, España.

VASAK, Karel (1982), *International Human Rights,* Vol. 1*,* Greenwood Press, San Francisco, EUA.

VINCENT, R.J. (1999), *Human Rights and International Relations*, Cambridge University Press, Cambridge.

Sitios consultados en Internet

Alto Comisionado de las Naciones Unidas para los Derechos Humanos. http://www2.ohchr.org/spanish/law/crc.htm

Carta de Derechos Fundamentales de la Unión Europea. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/union_europea/common/pdfs/B.1-cp--Carta-de-los-Derechos-Fundamentales.pdf

Convención Americana sobre Derechos Humanos. http://www.oas.org/Juridico/spanish/tratados/b-32.html

Convenio para la Protección de los Derechos y las Libertades Fun-

damentales.http://www.acnur.org/biblioteca/pdf/1249.pdf

Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf

Children´s Online Privacy Protection Act, 1998. http://www.ftc.gov/ogc/coppa1.htm

Preámbulo de la Declaración de los Derechos del Niño de 1959. Documento de Naciones Unidas A.G. res. 1386 (XIV), 14 U.N. GAOR Supp. (No. 16), p. 19, ONU Doc. A/4354 (1959). http://www.iin.oea.org/BADAJ2/pdf/Normativa%20ONU/Declaraci%C3%B3n%20de%20los%20Derechos%20del%20Ni%C3%B1o%201959.pdf

Declaración Universal de los Derechos del Hombre. http://www.un.org/es/documents/udhr/

Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf

Documento de trabajo 1/08 sobre la protección de datos personales de los niños, Unión Europea. https://212.170.242.196/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/2008/common/menores_es.pdf

El Universal. Lunes 28 de septiembre de 2009. 'Reclutadores de empleo buscan información en redes sociales'. http://www.eluniversal.com.mx/articulos/55885.html

Guidelines on Child Online Protection. Presentado en Unión Internacional de Telecomunicaciones el 5 de Octubre de 2009. http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

Ley Federal de Transparencia y Acceso a la Información Pública

(México). http://www.ifai.org.mx/

Nota informativa publicada por la Agencia Española de Protección de Datos del 15 de octubre de 2009. Barómetro de septiembre de 2009 del CIS. "La AEPD destaca la alta desconfianza de los ciudadanos españoles en la seguridad de sus datos en Internet". http://www.alfa-redi.org/noticias.shtml?x=11602

Opinión 5/2009 sobre redes sociales en línea del grupo de Trabajo de Protección de Datos de la Comisión Europea. http://ec.europea.eu/justice_home/fsj/privacy/index_en.htm

Página oficial de la Organización de Estados Americanos. http://www.oas.org/Juridico/spanish/tratados/b-32.html

Pacto Internacional de Derechos Civiles y Políticos. http://www.cinu.org.mx/onu/documentos/pidcp.htm

Recomendaciones 'Derechos de niños y niñas deberes de los padres y madres 2008'. España. http://www.ftc.gov/ogc/coppa1.htm

Resolución 45/95 de la Asamblea General de la Organización de las Naciones Unidas. https://www.agpd.es/portalweb/canaldocumentacion/legislacion/organismos_internacionales/naciones_unidas/common/pdfs/D.3BIS-cp--Directrices-de-Protecci-oo-n-de-Datos-de-la-ONU.pdf

Revista de derecho informático Alfa-Redi. http://www.alfa-redi.org/rdi.shtml

Revista Informador. http://www.informador.com.mx/tecnologia/2009/144861/6/filial-de-deutsche-telekom-pierde-datos-personales-de-clientes-estadounidenses.htm

Texto constitucional mexicano reformado. http://www.diputados.gob.mx/LeyesBiblio/

Tribunal Constitucional de España. Sentencia 292 del 30 de noviembre de 2000. http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=7467

Género e Internet

Florencia Barindelli[*]

Internet, entendida como un nuevo espacio social, recoge gran parte de las esperanzas y de los miedos actuales respecto al futuro. En la web se socializan las niñas y los niños, se reproduce o se cuestiona la discriminación, se difunde vieja violencia y se genera nueva. Este artículo revisa algunas tensiones centrales alrededor de Internet, la manifestación de las mismas en la teoría feminista y algunas de sus expresiones concretas en la vida de las mujeres y de los hombres. Asimismo, se busca enfatizar la relación internet y género para el caso de los más jóvenes, teniendo en cuenta la apropiación que ellos tienen de la tecnología y el impacto de ésta sobre las nuevas generaciones.

1. Internet y cambio social: tecnofóbicos y tecnofílicos

En los últimos años el número de usuarios y la cobertura de Internet en el mundo han aumentado exponencialmente. La can-

[*]La autora es Licenciada en Sociología por la Universidad de la República, Uruguay. Se desempeña como especialista en violencia sexual hacia niños, niñas y adolescentes en el Instituto Interamericano del Niño (OEA), donde actualmente coordina un observatorio sobre explotación sexual comercial infantil y adolescente. Ha sido consultora para diversos organismos internacionales y organizaciones sociales, tanto en su país como en la región.

tidad de usuarios de Internet en América ha crecido un 253.9% en el período 2000 – 2009. En diciembre del año 2009 se estimaban 446.483.050 usuarios de la red, lo que representa un 48% de la población del continente. La penetración de Internet es mayor en EE.UU. y Canadá, pero el aumento del acceso en las zonas con menor cobertura crece relativamente más rápido. La cantidad de usuarios en el Caribe ha aumentado 1549.8% en el período 2000 – 2009, siendo hoy la penetración de Internet en el Caribe similar a la de América Central (alrededor del 22.7%) y algo menor que en América de Sur, donde alcanza el 36.5% de la población.[1]

Otros cambios tecnológicos son igualmente significativos: el aumento del ancho de banda y de la capacidad de almacenamiento, el acceso inalámbrico a Internet especialmente a través de la telefonía móvil, las aplicaciones que permiten el intercambio de sonidos e imágenes de alta calidad en forma instantánea. También se ha revolucionado la forma en que los usuarios se comunican y crean contenidos: las redes sociales y las aplicaciones *peer to peer*,[2] habilitan el libre intercambio de información, el compartir todo tipo de archivos (texto, imágenes, audio) y la autogeneración de contenidos.

Nos encontramos frente a un nuevo escenario social que es interpretado desde puntos de vista contrapuestos. Tanto tecnofílicos como tecnofóbicos se basan en posiciones unidimensionales y producen discursos extremos.

Para los primeros, las TICs e internet son el medio para alcanzar resultados largamente deseados por la humanidad, que van desde una mayor y activa participación política hasta la emancipación de grupos oprimidos. Se le atribuye la posibilidad de dejar atrás la pobreza por medio del acceso a información estratégica de grandes contingentes de población corrigiendo "fallas" en el mercado de trabajo, y ha sido fuente de esperanza por ciertas características

[1]Datos de *Internet World Stats. Usage and Population Statistics*, actualizados al 31 de diciembre de 2009. Disponible en: http://www.internetworldstats.com/stats2.htm

[2]"Forma coloquial de referirse a las denominadas redes entre iguales, redes entre pares o redes punto a punto. En estas redes no existen ni ordenadores cliente ni ordenadores que hagan de servidor. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre los ordenadores interconectados". (Fuente: Wikipedia)

supuestamente intrínsecas a la red: su carácter abierto, difuso y no jerárquico, o su tendencia a la cooperación entre los distintos actores.

Los tecnofóbicos ven a internet como una catástrofe. Argumentan que las TICs e internet no hacen más que perpetuar viejas formas de dominación y hegemonía cultural; que no son más que un medio para que la elite continúe reproduciendo su poder económico, político y cultural, pero encima ahora por un medio que además vigila y controla a los usuarios del planeta.

2. Expresiones en la teoría feminista acerca de estos dilemas

Estas posturas dicotómicas pueden rastrearse – a veces en forma expresa y otras veces no – en la relación género y TICs. Así, con mucho optimismo, hubo corrientes feministas en la década de los noventa que concibieron al entorno virtual como una oportunidad política para el logro de la equidad de género.

La virtualidad ofrece la posibilidad a la mujer de "liberarse" del cuerpo, haciendo posible una interacción más igualitaria y libre. Esta idea, que ya Shulamith Firestone argumentaba en 1972,[3] adquiere gran influencia una vez que Donna Haraway acuña el término "*cyborg*", como *"un organismo cibernético, un híbrido de la máquina y el organismo*",[4] tanto natural como artificial, tanto femenino como masculino.

Al liberarse del cuerpo, de la biología, también puede experimentar en forma creativa con su identidad. La corriente denominada 'Ciberfeminismo' explora el problema de la identidad y la sexualidad en el ciberespacio. Sherry Turkle,[5] afirma que internet permite las subjetividades múltiples y fluidas (jugar a ser otro/a) cuestionando la concepción moderna de una única identidad.

[3]*Cfr. The Dialectic of Sex*.

[4]D. Haraway, "A manifesto for cyborgs: science, technology and socialist feminism in the 1980's". Publicado inicialmente en *Socialist Review*, 80 (1985), y recogido como "A Cyborg Manifesto" en *Simians, Cyborgs and Women: The Reinvention of Nature*, Free Association Books, London, 1991. Citado en Sanz González, 2006.

[5]S. Turkle (1995), *Life on the Screen: Identity in the Age of the Internet*, Simon & Shuster, New York. Citado en Sanz González, 2006.

También se destacan características o cualidades valoradas en la red que se ajustarían a ciertos "caracteres femeninos", como ser la centralidad de la comunicación y la cooperación o la habilidad para realizar varias tareas al mismo tiempo.[6]

Estas autoras han sido criticadas por sus posturas esencialistas respecto a la mujer y lo femenino; es decir, que aceptan la existencia de determinadas características como dadas a la mujer en forma inmutable. Se trata de características que han servido históricamente a la exclusión de las mujeres y que se retoman, valorizándolas positivamente, por las corrientes esencialistas. Pero además, estas autoras han sido criticadas por su esencialismo respecto a las tecnologías digitales. Comparten lo que en filosofía se ha denominado *determinismo tecnológico:*

> "[…] consiste en la creencia en la inevitabilidad de los desarrollos tecnológicos y la idea de que afectan a la sociedad pero ésta no influye en sus desarrollos. Esta concepción tiene como consecuencia la ausencia de análisis y crítica al modo en que se producen los artefactos tecnológicos. El determinismo tecnológico en general potencia una postura más bien inmovilista en cuanto a los dilemas éticos y políticos en el ámbito de la tecnología […]" (Sanz González 2006: 198).

El determinismo tecnológico deja pasivos a los individuos; no solo al movimiento feminista. Y, lamentablemente, es una concepción más frecuente de lo que parece a simple vista, ya que se encuentra solapada en muchos discursos que construyen opinión: en editoriales, en informes temáticos que circulan en los medios de comunicación, incluso en argumentaciones políticas o en el medio de discusiones legislativas.

El determinismo tecnológico está presente cada vez que se asume una nueva invención tecnológica como un ovni descontextualizado, como algo que "llegó" a la humanidad y que la humanidad debe ver ahora cómo hace para sacarle provecho. Incluso no son pocas las ocasiones en las que los intentos de situar la creación tecnológica en su tiempo histórico y por ende, en la trama de relaciones de poder que en constante pugna rodean cada invención tecnológica, son desacreditadas como posturas tecnofóbicas.

[6] S. Plant, *Zeros and Ones: Digital Women and the New Technoculture*, Fourth Estate, London, 1998. Citado en Sanz González, 2006.

Como señala Jesús Martín-Barbero, las tecnologías no son meras herramientas transparentes, y no se dejan usar de cualquier modo, son la materialización de una cultura y de un modelo global de organización del poder.[7]

En cuanto a la relación específica entre género y TICs, si las tecnologías digitales fueran inherentemente femeninas y liberadoras, no sería necesaria la acción política ni un cambio en la estructura profunda de la sociedad, ya que sería la misma tecnología la que estaría produciendo la igualdad. A este tipo de posturas se las llama "tecno-optimistas" porque presuponen que el desarrollo tecnológico conduce inevitablemente al progreso social y, por esta misma razón, en general rechazan cualquier intromisión institucional en lo que pretenden sea "una sociedad libre de regulaciones" (Sanz González 2006: 199).

También existen voces desde el feminismo que relacionan el avance tecnológico con un empeoramiento relativo de la situación de las mujeres. Estas voces se centran en la brecha digital de género, en las posibilidades que tiene internet para magnificar los estereotipos discriminatorios y los alcances de ciertos tipos de violencia y de violación de derechos, y en la baja participación de las mujeres en el diseño y la producción industrial de la tecnología, que las vuelve a colocar en los últimos peldaños de una industria pujante o en meras consumidoras.

Sea cual sea la postura, *"lo común de ambos argumentos es el reconocimiento de que las tecnologías de información no son meros recursos o instrumentos que se insertan en un orden socioeconómico y cultural preexistente sino que lo subvierten, aunque de maneras altamente complejas y todavía poco exploradas*" (Bonder, 2008: 919).

[7] Jesús, Martín-Barbero (1987), *De los medios a las mediaciones*, Convenio Andrés Bello, Editorial Gustavo Gili, S.A., Barcelona, España. Citado en Bonder, 2008:931.

3. Internet como un nuevo espacio social

Manuel Castells es uno de los principales exponentes de la denominada "sociedad de la información". Junto a otros pensadores contemporáneos, ubica a internet como la nueva base material sobre la que giran los procesos económicos, políticos y sociales de los últimos años. Son ya famosas sus palabras al inicio del Doctorado sobre la Sociedad de la Información y el Conocimiento (2001): *"Internet es el tejido de nuestras vidas en este momento. No es futuro. Es presente. Internet es un medio para todo, que interactúa con el conjunto de la sociedad y, de hecho, a pesar de ser tan reciente, es su forma societal".*

La imbricación entre internet y todos los aspectos de la vida social – las formas de relacionamiento social, las representaciones imaginarias y simbólicas, las percepciones y legitimaciones sociales, los futuros a los que aspiramos con miedo u esperanza, etc. – sería tal, que habría una co-construcción entre relaciones sociales y tecnología y no sería posible analizar unas sin la otra.[8]

El denominado 'Tecnofeminismo',[9] incluye la categoría género como una variable explícita de análisis en la co-construcción entre tecnología y sociedad. "*La tecnología no sólo «afecta» a las relaciones y a la definición de género, sino que, afirman, en toda innovación tecnológica se produce una renegociación de las relaciones y una articulación de las identidades de género que van a ser performadas con el uso de ese artefacto"* (Sanz González, 2006:194).

Estas autoras consideran que cada nueva renegociación no se realiza entre iguales, sino entre actores inmersos en una estructura de poder discriminatoria para las mujeres que se genera y perpetúa por el proceso mismo de representarse como tales en las acciones sociales. La construcción de género es un proceso performativo:[10] se es mujer o varón porque se actúa como mujer o varón. Se trata de

[8]Tampoco cabe entender que las relaciones sociales son producidas por la tecnología.

[9]Como denomina Judy Wajcman a la intersección entre feminismo y constructivismo: *"la corriente de CTS (Ciencia, Tecnología y Sociedad) que subraya la contingencia y la heterogeneidad del cambio tecnológico, que se localiza a su vez dentro de redes sociales más amplias, pero introduciendo un espacio para la agencia de las mujeres dentro de los cambios tecnológicos"* en J. Wajcman, *Technofeminism*, Polity Press, Cambridge, UK, 2004, p. 7. Citado en Sanz González, 2006.

[10]*Cfr.* J. Butler (1990).

un comportamiento (actitudes, acciones y estereotipos) aprendido y repetido desde la infancia. Sentimos, pensamos y actuamos como seres generizados; esto también es así en las redes tecnocientíficas.

Una mirada constructivista no es tecnofóbica; ni siquiera pesimista. Las predicciones sobre los efectos grandiosos o terribles de internet, no toman en cuenta el enorme margen de variabilidad que tiene internet, ni la incidencia que tanto productores como usuarios ejercen sobre esa variabilidad. Citando nuevamente a Jesús Martín – Barbero en Bonder (2008:929), *"internet no es solamente un medio de comunicación, sino que es un nuevo espacio social"*.

4. Las mujeres en el nuevo espacio social de Internet

Respecto al tema género e internet hay numerosos estudios que, desde distintos enfoques teóricos y metodológicos, buscan iluminar partes del fenómeno.

Por un lado, encontramos las investigaciones de carácter cuantitativo que analizan la cantidad de mujeres con respecto a los hombres en diversos sectores de las TICs. Estos estudios,[11] se centran en cuántas mujeres y cuáles mujeres acceden a internet y qué consumen en internet.

En Estados Unidos el porcentaje de mujeres que usan internet está apenas por debajo que el porcentaje de hombres, salvo en los grupos de mujeres menores a 30 años y en las mujeres de raza negra. En estos grupos, las mujeres superan a los hombres en el uso de internet. Contrariamente, las mujeres con más años están muy atrás en el uso de internet en comparación con los hombres mayores (Fallows, 2005).

Los hombres usan internet más intensamente que las mujeres: están más tiempo online y suelen contar con banda ancha. También realizan más transacciones; si bien tanto hombres como

[11]Ejemplos citados en Sanz González son: G. Lovegrove y B. Segal. (1991), *Women into Computing: Selected Papers 1988-1990*, Springer-Verlag, London & Berlin; R. Lander, y A. Adam (1997), *Women in Computing*, Intellect, Exeter, UK; y en Estados Unidos por ejemplo Tracy Camp (1997), "The Incredible Shrinking Pipeline", *Communications of the ACM*, vol. 40, no.10, pp. 103-110.

mujeres están igualmente dispuestos a comprar y hacer uso del e-banking, son los hombres quienes suelen pagar sus cuentas, participar en remates, comprar y vender bonos y acciones y pagar por contenidos digitales. También usan más internet como un medio para la recreación: recolectan información respecto a sus hobbies, toman clases, bajan música y videos, escuchan radio, leen libros y artículos en las pantallas (Fallow, 2005).

Las críticas que suelen hacerse a estos estudios cuantitativos es que en general carecen de una reflexión acerca de las causas de estas diferencias, por lo que se ciñen políticamente a las propuestas de igualdad formal.

Por otro lado, encontramos estudios que se dedican a averiguar si hombres y mujeres tienen diferentes actitudes frente a problemas concretos que provocan las TICs,[12] llegando a la conclusión que las mujeres se preocupan más por temas como la responsabilidad social y el medio ambiente. Estas aproximaciones caen en el esencialismo femenino que no toma en cuenta los estereotipos culturales de género en los que las mujeres son socializadas (Sanz González, 2006: 200-201).

Respecto al uso de determinados medios como el correo electrónico, se ha identificado que las mujeres lo usan para nutrir sus relaciones afectivas, mientras que los hombres lo usan más como medio para transmitir y recibir información de un rango variado de organizaciones (Fallow, 2005). De manera similar, las adolescentes utilizan el chat como forma de estar en contacto permanente con sus amigas y amigos, para alimentar sus relaciones cercanas, incluyendo aquellas con los amigos de amigos.

Una crítica que han tenido este tipo de estudios, es que llegan a conclusiones aparentemente categóricas, pero que para llegar a ellas deben uniformizar la realidad y dividirla en dos categorías supuestamente excluyentes: hombre – mujer. Es así que no se visualizan las diferencias internas que tienen, las superposiciones ni las relaciones entre ellas.

[12]Ejemplos citados en Sanz González son: D. Khazanchi, "Unethical behavoir in information systems: the gender factor", *Journal of Bussiness Ethics*, nº 15, 1995, pp. 741-749, o E. Mason y P. Mudrack, "Gender and ethical orientation: a test of gender and occupational socialization theories", *Journal of Bussiness Ethics*, nº 16, 1996, pp. 599-604.

Otra línea de estudios comparativos tiene que ver con los tipos, la cantidad y la calidad del empleo de las mujeres en el sector de las TICs y su escasa incidencia en los puestos de poder de esta industria.

Finalmente, existen estudios que buscan comprender las experiencias de las mujeres en la red, en particular buscando contrastar la hipótesis de que las TICs contienen la posibilidad de revertir los patrones de género existentes en el mundo offline. Estos análisis se centran en aspectos tales como las diferencias de estilo en la comunicación de hombres y mujeres, en las diferencias en la construcción de la propia imagen y en las imágenes y valores que se transmiten a través de internet, en particular a través de los videojuegos para niños y niñas.

Los varones se imponen en la comunicación en los espacios mixtos, son quienes introducen más temas nuevos e ignoran o trivializan los planteados por las mujeres, inician y finalizan las discusiones, plantean sus puntos de vista como hechos comprobados, se atreven a usar lenguaje vulgar o insultos y a confrontar a los interlocutores. Las mujeres son menos agresivas y tienden a enviar mensajes más personales, a atenuar las afirmaciones, a disculparse y a expresar apoyo, acuerdo o consideración a sus interlocutores. Ellas valoran más las reglas y se molestan más cuando éstas no se respetan; de hecho participan más de los espacios donde hay moderadores, incluso si los espacios son de formación. Las reglas y alguien a cargo de hacerlas cumplir parece darles las garantías para una interacción más equilibrada y sobre todo librarse de las amenazas de acoso, de las continuas interrupciones masculinas y de su tendencia a monopolizar la conversación (Bonder, 2001:11-12).[13]

[13]La autora se basa en diversos estudios para llegar a estas afirmaciones, ellos son: Susan Herring, *Gender and participation in computer-mediated linguistic discourse,* Washington, D.C.: ERIC Clearinghouse on Languages and Linguistics. Document No. ED345552, 1992 y "Gender and democracy in computer-mediated communication", http://www.cios.org/www/ejc/v3n293.htm, *Electronic Journal of Communication* 3(2), 1993. "Two variants of an electronic message schema" en S. Herring (ed.), *Computer-Mediated Communication: Linguistic, Social and Cross-Cultural Perspectives*. Amsterdam: John Benjamins Publishing Co., 1996a; C. Kramarae y J. Taylor, "Women and men on electronic networks: A conversation or a monologue?" en H.J. Taylor, C. Kramarae y M. Ebben (eds.), *Women, Information Technology, and Scholarship*, Urbana, IL: Center for Advanced Study, 1993; V. Savicki *et. al., Op. cit.,* "Gender language style and group composition in Internet discussion groups", *Journal of Computer- Mediated Communication* 2(3),

Cuando se comparan los perfiles en las múltiples redes sociales o la imagen a transmitir por medio de los blogs o páginas personales, resulta que las mujeres tienen más dificultad para exhibir sus competencias y promocionar su conocimiento, necesitando mostrar todos sus méritos y honores e incluyendo datos de su vida personal, mientras que los hombres enfatizan en el diseño su estatus, sus capacidades y competencias. Las chicas suelen presentarse como agradables y atractivas y utilizan colores pastel y dibujos florales.

Como señala Bonder (2001): "*El conjunto de datos presentados hasta acá parece darle la razón a quienes afirman que más allá de estar peleando la batalla por el acceso, las mujeres no hemos avanzado mucho en dejar impresas otras huellas en la autopista informática más allá de las previstas para nuestro género".*

5. Niños, niñas, adolescentes y jóvenes en Internet: los verdaderos actores del nuevo espacio social

Respecto a la exposición de los niños, niñas y adolescentes a las TICs también se escuchan discursos extremos: o bien Internet es la puerta al mundo, la vía regia al desarrollo integral y a la inclusión social de los más chicos, o bien Internet es fuente de temores y amenazas que, en general, son difíciles de explicar por los adultos. Son difíciles de explicar no porque los riesgos no existan, sino porque "brecha generacional" mediante, los adultos desconocen básicamente lo que los niños hacen en Internet y, por lo tanto, sus temores se expresan en términos absolutos, con poca fundamentación y pocos recursos para abordar la situación. Frente a la impo-

1996; L. Sutton, *Using Usenet: Gender, power, and silence in electronic discourse.* Proceedings of the 20th Annual Meeting of the Berkeley Linguistics Society. Berkeley: Berkeley Linguistics Society, 1994. K. Hall, *Op. cit.*, 1996; S. Herring, "Posting in a different voice: Gender and ethics in computer-mediated communication" C. Ess (ed.), *Philosophical Perspectives on Computer-Mediated Communication*, Albany: SUNY Press. 1996b.: L. Colin-Jarvis, *Discriminatory messages and gendered power relations in on line discussions groups*, Presentación en Encuentro Anual de la National Communication Association, Chicago. IL. 1997; M. Ebben, *Women on the Net: An Exploratory Study of Gender Dynamics on the soc.women Computer Network*. Unpublished doctoral dissertation, University of Illinois at Urbana Champaign. 1994; E. Reid, *Cultural Formations in Text-Based Virtual Realities*, Master's thesis, University of Melbourne, Australia.

tencia y el desconocimiento, los padres oscilan entre la confianza ciega y la desconfianza-prohibición excesiva.

Sucede que en este nuevo espacio social, los más jóvenes se sienten en casa. Marc Prensky (2001) plantea, de manera provocadora, la distinción entre nativos e inmigrantes digitales: los primeros, son las personas para las cuales la tecnología digital ha sido su entorno de socialización y los segundos, son aquellos que se han tenido que adaptar a un nuevo lenguaje pero que piensan y procesan la información en forma fundamentalmente diferente a los "nativos".

Digo en forma "provocadora", porque de esta categorización se desprende una distancia entre generaciones de carácter cognitivo que según Prensky obliga a repensar parte de los contenidos educativos y principalmente la metodología educativa. *"Different kinds of experiences lead to different brain structures", says Dr. Bruce D. Perry (…) … it is very likely that our students´ brains have physically changed (…) But whether or not this is literally true, we can say with certainty that their thinking patterns have changed"* (Prensky, 2001:1).

Estos cambios en las formas de pensar, ¿tienen algo que ver con el género?

En la comunicación en los chats, donde se ha verificado una participación más igualitaria en cuanto a la extensión de los mensajes y a la cantidad de mensajes, los *nicknames* no funcionan como máscaras que ocultan completamente el género. La pertenencia genérica se nota en el uso de pronombres en tercera persona, en la misma elección del apodo, en el uso de vocablos e íconos. Los varones alteran más las normas gráficas, reducen las palabras y son más esquemáticos. Las chicas usan un vocabulario con expresiones coloristas, refieren a verbos afectivos como abrazar, son más formales con el idioma.

Como señala Bernárdez Rodal, la creatividad e invención para crear signos de identidad común interviniendo en el lenguaje, incluyendo íconos y demás, "*está determinada por la utilización de signos y códigos estereotipados sobre todo en lo que se refiere al sexo".* Los adolescentes no renuncian a las formas generizadas de hablar, estando la determinación de género incluida en las interacciones lingüísticas a través de internet.

"Si aceptamos estas conclusiones, aceptamos un argumento sencillo: que los textos que se producen en Internet son continuadores de la tradición lingüística y su estructura de género (Baron, N. S: 2004)", (Bernárdez Rodal 2006:76).

Dado que nos presentamos a través del código común del lenguaje y difícilmente los y las adolecentes puedan y quieran revolucionar el modo de hablar masculino y femenino ya estipulado y que se efectiviza en los ejemplos que dimos anteriormente: lenguaje asertivo masculino, turno de la palabra, vocabulario, etc. Si las personas estructuran aquello que les es significativo a partir de su relación con el mundo circundante, lo que viven en internet es parte del "camino a la cultura".

6. Internet como espacio de juego

Algunas de las destrezas de los niños, las niñas y los y las adolescentes actuales – o de una creciente cantidad de ellos – son su capacidad para recibir información más rápidamente, de procesar varios temas o asuntos en paralelo, de acceder al conocimiento desde distintos puntos o en forma "desordenada" y no siguiendo el tradicional modelo de aprendizaje sistemático y paso a paso. Trabajan en red y parecen necesitar recompensas o gratificaciones en forma más frecuente (Prensky 2001:2).

La lógica del juego – y del videojuego – moldea sus habilidades y capacidades para adquirir conocimiento y para integrarse a la cultura. Algunas de las fortalezas que, según Saz Rubira (2004) tienen los videojuegos son las siguientes:

- Son apropiados para el desarrollo de habilidades visomotoras, lateralidad, y organización espacial y temporal.

- Favorecen la repetición instantánea y continua hasta dominar la situación, adquiriendo la sensación de control.

- Son una de las entradas más directas a la cultura informática y a la cultura de la simulación.

- Son muy seductores y motivadores en sí mismos.

- Permiten aprendizajes encubiertos que salvan la resistencia a los aprendizajes formales.

- Facilitan el ejercicio de la fantasía.

Pero no son solamente "los niños de ahora" los que aprehenden el mundo por medio del juego. Jugando los niños ejercitan sus funciones motoras y psicológicas mientras descubren y miden la evolución de sus aptitudes. Se descubren a sí mismos investigando sus potencialidades corporales y psíquicas, así como su contexto simbólico y material.

Dice Winnicott (1990): "*El jugar tiene un lugar y un tiempo…No se encuentra "adentro" (…) tampoco está "afuera". (...) Jugar es hacer (...) Es bueno recordar siempre que el juego es por sí mismo una terapia. (...) En él, y quizá sólo en él, el niño o el adulto están en libertad de ser creadores".* El juego es fundamental en el proceso de diferenciación y en el desarrollo de la conciencia de sí mismo, ya que crea un espacio intermedio que origina la experiencia cultural.

Por medio de la ficción del juego, el niño comienza a introducir en su vida psíquica el simulacro, es decir la ligazón entre el indicio (unido a aquello que se representa) con el símbolo (conexión mental discursiva). Al tomar fuerza el pensamiento simbólico y la representación, consigue distanciarse progresivamente de la realidad. En la medida que los niños son capaces de abstraer más pueden darle nuevos significados a sus vivencias (Araújo, 2000). En el juego se integran, entonces, los aspectos afectivos, intelectuales, sociales y motores del desarrollo.

Vale la pena detallar algunas de las características generales del proceso de socialización de los niños señaladas por Ferrán Casas (1998):

a. las experiencias precoces dejan huellas permanentes en las personas;

b. son las propias pautas sociales – sus normas, imágenes y valores – las que orientan cómo socializar al niño;

c. la socialización es adaptativa: se trata de un aprendizaje que le permite a cada niño integrarse a un grupo más amplio;

d. la socialización es anticipativa: prepara a cada niño para el status de edad subsiguiente.

El proceso por el cual los individuos – en especial los niños – interiorizan la estructura social (socialización), se lleva a cabo en los distintos espacios sociales en los que se interactúa: uno de ellos, cada día más importante, es internet. "*Por primera vez en la historia, la generación de chicos actuales, nacidos entre medidos de los noventa y principios del año 2000 se están introduciendo a/en los medios (la cultura, el mundo, la subjetividad) a través del intermediario digital (…)*" (Piscitelli, 2006: 182).

Es muy ilustrativo el inicio del artículo de Bernárdez Rodal (2006:69) que comienza con la descripción de un lugar y de lo que algunas personas hacen, sienten y piensan durante sus primeros minutos en ese lugar. El lugar es Habbo Hotel, un "*ciber-lugar específicamente creado para que los y las adolescentes tengan un espacio donde interactuar; un lugar que consideren como propio, que les divierta, que puedan construir a su medida, donde poder estar juntos con cierta intimidad",* y las personas descriptas son adolescentes de distinto sexo y edad que han elegido previamente sus cuerpos virtuales y han ingresado al espacio de interacción que les ofrece Habbo Hotel.[14]

En la última década se han desarrollado muchas aplicaciones en las que jugar es vivir; es transitar, interactuar y crear en una virtualidad que simula la realidad. Por ejemplo en "Second life",[15] como su nombre lo indica, cada usuario o residente está en continuo contacto con los demás avatares.[16] La comunicación puede ser vía chat, vía mensaje instantáneo o voz; se participa de diversas actividades donde encontrarse con amigos residentes o conocer nuevos: desde ir a un bar a escuchar buena música hasta viajar a territorios virtuales desconocidos. Es posible crear el avatar, modificar su aspecto y su conducta, crear la casa donde vive, su jardín, la forma en que baila, etc. También es posible comerciar servicios y propiedad virtual.

[14]http://www.habbo.es/community

[15]Los adolescentes entre 13 y 17 años pueden jugar en *Teen Second Life* (http://teen.secondlife.com/), en donde los adultos no pueden ingresar. Respecto a las posibilidades reales de controlar la edad de quienes navegan por determinados sitios hay una fuerte discusión a nivel internacional.

[16] *"An avatar is a computer user's representation of himself/herself or alter ego whether in the form of a three-dimensional model used in computer games, a two-dimensional icon (picture) or a one-dimensional username used on Internet forums and other communities, or a text construct found on early systems such as MUDs. It is an object representing the user. (…) This sense of the word was coined by Neal Stephenson in 1992 novel Snow Crash, who co-opted it from the Sanskrit word avatāra, which is a concept similar to that of incarnation".* (http://en.wikipedia.org/wiki/Avatar_%28computing%29). *Cfr.* también http://wiki.secondlife.com/wiki/Avatar/es

Se trata de espacios de experimentación en los que los y las adolescentes arman y actualizan la imagen que tienen de sí mismos, estructuran qué es lo que tiene sentido para ellos y ensayan diversos roles sociales.

7. Internet como espacio para la construcción del sí mismo

El aporte que realiza Erving Goffman, desde la teoría sociológica, a la comprensión de la interacción cara a cara, es útil para nuestra discusión acerca de la construcción de sí mismo en internet.

La acción social es una acción ubicada en un contexto, y su sentido debe comprenderse en relación con la situación interactiva en la que surge. Esta situación interactiva es ordenada; sigue reglas, normas y rituales. Se trata de un orden que se basa en las convenciones sociales (contrato social) y en los principios y valores aceptados como buenos y justos (consenso social) (Herrera Gómez, M. y Soriano Miras, R.M., 2004:61).

Otra característica de las acciones sociales es que son siempre comunicativas, ya que tienen como finalidad la presentación de sí mismo de cada uno de los actores presentes en la situación. Las personas hacen un gran esfuerzo por elaborar y mantener su propia fachada personal, ya que las informaciones "incorporadas" en elementos físicos (apariencia) hablan del perfil de persona que se quiere transmitir y de la consecuente impresión que se quiere provocar en los demás.

La fachada proyectada por el actor no es aleatoria, arbitraria o atemporal, sino que es "un equipamiento expresivo de tipo estandarizado"; está compuesta por atributos que ya cuentan con el consenso social. Justamente la definición adecuada de la situación y, por

tanto, la adopción de la fachada adecuada para esa situación, es una de las claves del proceso de socialización del que antes hablábamos.

Hay situaciones que están más predeterminadas que otras, claro. Las personas gestionamos disciplinadamente nuestra fachada y pretendemos que los demás (la audiencia) la tomen en serio. "*Por tanto, la acción social siempre es* performance*, representación para un público, y esto constituye un aspecto esencial de su "sentido" social"* (Herrera Gómez, M. y Soriano Miras, R.M., 2004:63).

En principio podríamos pensar que la interacción a través de internet sería menos comprometida que la interacción cara a cara, puesto que hay parte de la información que puede esconderse o porque el manejo del nivel de exposición es grande, puesto que cada emisor decide si agrega por ejemplo imágenes o video a sus perfiles, links o datos personales; incluso al usar herramientas más interactivas como la conversación, puede decidir si la misma será solo escrita, o si agrega voz y cámara.

Esta posibilidad de "dosificar" o de desplegar en forma más controlada, señales de presentación de sí mismo, es muy atractiva tanto para los usuarios como para las teorías que se desarrollan alrededor de estos fenómenos. Por un lado, por la libertad y la experimentación – por ejemplo eligiendo otros cuerpos virtuales, eligiendo los *nicknames*, personalizando sus perfiles, etc. – que en particular han destacado aquellas personas pertenecientes a grupos en desventaja o que sufren la discriminación por diversos motivos. Por otro lado, esta misma característica permite que una "falsa" identidad pueda utilizarse para engañar y perjudicar o dañar a otra persona, siendo el fraude, el anonimato, el robo de identidad *online* y el *grooming*, motivos de mucha preocupación actualmente.

Pero el sentimiento de libertad – impunidad no se da solamente en situaciones tan extremas; también tienen que ver con la presión o la obligación de "presencia" o de dar de uno mismo que tiene la interacción cara a cara. Los niños son muy claros cuando dicen sentirse más libres en internet porque por ejemplo pueden chatear y al mismo tiempo estar navegando en un sitio de interés o chateando con otra persona. Si estuvieran charlando y no chateando, sería muy grosero estar simultáneamente hablando con otro, leyendo un libro y comiendo. También el comienzo y la finalización de la interacción son más fáciles y sin mayor preámbulo.

Sin embargo, podemos preguntarnos junto con Bernárdez Rodal, ¿por qué, si el ciberespacio es un lugar privilegiado para prescindir del cuerpo, se "engaña" tan poco? "*Cuando entramos en los chat y observamos las conversaciones que allí tienen lugar, veremos sobre todo cómo los y las adolescentes hacen un gran esfuerzo, primero, por controlar la imagen que proyectan de sí mismos, y segundo, por interpretar de forma adecuada las informaciones sobre los datos que ofrecen los demás, porque, al fin y al cabo, construirse una identidad atractiva en la red, parece una tarea casi tan laboriosa como puede serlo en las interacciones cara a cara"* (2006:78).

Esta "oportunidad liberadora" de la que ya se ha hablado – sin dejar de tener sentido, al igual que los riesgos antes mencionados – no es necesariamente la manera prioritaria en que es vivida la interacción en internet por los "nativos digitales". Ser popular, creativo, ocurrente, raro, *cool, nerd*, divertido, tímido, y la multitud de atributos consensuados existentes para definir o presentar a la persona, tienen sentido para las niñas, los niños y las y los adolescentes tanto en la interacción cara a cara como en la virtual.

¿Por qué? En primer lugar, porque gran parte de la interacción por internet se realiza con personas conocidas o conocidos de conocidos (significativos) para los niños, niñas y adolescentes.[17] Parte de la interacción responde a una suerte de continuación entre un espacio y otro. En segundo lugar, porque para los chicos que están inmersos y pasan gran parte de su día y su vida en internet, la web es un ámbito más de socialización, un ámbito más en donde se definen a sí mismos y a las situaciones por las que transitan. (Que sea un ámbito más no quiere decir que sea igual, pero sí que es relevante y que por tanto el esfuerzo por presentar un sí mismo positivo o agradable, vale la pena).

También hay razones tecnológicas. Las características de la ya antigua "revolución 2.0" promueven, fomentan y obligan a la presentación del sí mismo. El usuario es el centro del diseño y es productor de contenidos; el usuario interactúa directamente con otros usuarios y las aplicaciones cuentan con interoperatividad para facilitar este intercambio, cooperando tanto los usuarios como las

[17] *Cfr.* Elisheva F. Gross (2004), "Adolescent Internet use: What we expect, what teens report", *Journal of Applied Developmental Psychology* (25), pp. 633-649. Citado en Bernárdez Rodal, 2006:77.

computadoras unas con otras. Existe una creciente interactividad e instantaneidad, además del aumento en el acceso y en la posesión de artefactos tecnológicos.

En especial en los países desarrollados no es extraño que un niño, niña o adolescente sea "el dueño" de más de un artefacto electrónico, todos ellos interconectados entre sí y todos respondiendo al mismo usuario. Para los nativos digitales no tiene sentido estar abriendo una y otra vez sesiones, cortando y pegando comentarios en distintas aplicaciones, guardándose archivos y andarlos transportando físicamente de un artefacto a otro, etc.[18]

También están las limitaciones lingüísticas. Como hemos visto, al utilizar el código simbólico de las palabras, mucho decimos de nosotros mismos, además de lo que explícitamente estemos intentando expresar en forma literal.

Entonces, la interacción presupone una definición de la situación por parte del actor y una búsqueda por presentarse a sí mismo de determinada manera, y tanto la situación como los elementos para presentarse que utiliza el actor lo anteceden, son socialmente construidos. Los niños, las niñas y adolescentes al interactuar en internet no "engañan" demasiado, en parte porque no les interesa y en parte porque no pueden.

Como señala Herrera Gómez, M. y Soriano Miras, R.M., (2004:63) "*el actor jamás es del todo consciente y «dueño» de la propia performance. Por eso distingue [Goffman] entre las comunicaciones que el actor trasmite intencionalmente y las expresiones que «deja entrever»* (1959:12-17)".

[18]Como se dijo anteriormente, no estamos afirmando que en la actualidad esta descripción sea ajustada a la mayoría de los niños, niñas y adolescentes en América Latina. Aún frente a la reducción de la brecha digital y al aumento del consumo de tecnología digital, las capacidades de apropiación y las oportunidades que realmente pueden proporcionar las tecnologías, son muy variadas según la clase social, el capital cultural y el género.

8. Percepción por parte de los y las adolescentes y jóvenes de las diferencias de género en el ámbito de las TICs

A partir del trabajo en grupos focales con jóvenes participantes de 12 programas sobre "jóvenes y TICs" en América Latina, la investigación liderada por Bonder (2008) llega a las siguientes conclusiones: a) la mayoría de los jóvenes no reconocen la existencia ni las consecuencias de la discriminación de género en las TICs; b) la minoría que advierte la discriminación se divide entre quienes la consideran natural y quienes la cuestionan críticamente; c) no es un tema que les preocupa o que les motiva para involucrarse en cambiarlo; d) consideran innata la facilidad para el manejo de la tecnología de los chicos varones; e) las chicas que se destacan son consideras excepcionales y distantes del estereotipo femenino, tanto por sus habilidades tecnológicas como por su falta de interés en el coqueteo o apariencia física.

En el estudio citado, expresaron los siguientes intereses y modalidades en el uso de las TICs según género:[19]

Mujeres:

- Les atrae el uso de las TIC para las relaciones interpersonales y sociales. También les importa informarse y tratar cuestiones políticas y artísticas y la realización de actividades que puedan proveerles beneficios personales y a sus familias.

- Son más equilibradas en el manejo del tiempo dedicado al uso de las TIC, pero curiosamente ello no se valora claramente, sino que se atribuye a una limitación, el que tengan que ocuparse de las tareas domésticas, como una responsabilidad natural de su género *("tienen que hacer más cosas que el hombre y no pueden dedicarse todo el tiempo a eso*").

- Pueden ser más lentas o tener más dificultades al principio, pero cuando adquieren experiencia en el uso de las tecnologías suelen ser más rigurosas y capaces que los varones, en opinión de algunos.

Varones:

- Mayoritariamente se interesan por los videojuegos en los

[19]Transcripción de hallazgos Bonder, 2008: 927-928.

que "*ponen más la pasión, la adrenalina, la cosa de ser rápidos*". Están más absorbidos por la máquina, llegan a comportarse "*como un vegetal*", concurren con mayor frecuencia a los *cyber* y son habilidosos en el manejo del *hardware.*

- "*A los chicos les gusta descomponer cosas. Mirar adentro, a ellas no les gusta ensuciarse las manos". "Ellas les temen a las descargas eléctricas*".

Tanto las chicas como los chicos participantes de estos programas buscan por medio de ellos ampliar sus redes de interacción y comunicación, logrando la pertenencia a grupos, aumentar sus oportunidades laborales, económicas y de autonomía, adquirir conocimientos por medio de capacitaciones cortas y baratas (certificación a bajo costo) y sentirse en "la cresta de la ola" de un proceso global que augura un futuro posible y deseable (Bonder, 2008:926).

Claro que no es lo mismo saber qué buscan los adolescentes al participar en un programa específico sobre TICs, que averiguar qué es lo que buscan en su interacción cotidiana a través de internet. Sin embargo, hay algo que tienen en común los y las adolescentes, aún de diferentes niveles socioeconómicos. Según Bernárdez Rodal, "*la necesidad que tiene todo y toda adolescente de crearse "un entorno propio", una "personalidad" y una "identidad" determinada*" (2006:71).

Un entorno propio donde las personas de la misma edad se reconocen entre sí. Gran parte de los comportamientos de los adolescentes se explican por estar en un momento de la vida en la que están desarrollando su identidad individual junto a sus pares. Es el grupo de pertenencia, el grupo de pares, una referencia primordial, que tanto por identificación u oposición, comienza a tener fuerza en el desarrollo de la personalidad individual de los y las adolescentes.

Lo común y constante en la interacción de los adolescentes a través de Internet es la no presencia de adultos, en particular de los padres. Internet sustituye en parte o tiene un rol muy similar – aunque tenga particularidades obviamente – a "la plaza", "la calle", "la esquina":[20] ese lugar público donde los mayores no dominan la

[20]Lugar que, además, es percibido crecientemente por los adultos como un lugar dañino y peligroso.

interacción y donde los adolescentes sociabilizan y se definen a sí mismos en conjunto a su tribu, a su banda, a sus iguales.

¿Por qué los y las adolescentes deberían estar dispuestos a alejarse de las determinaciones de género? *"No hay que olvidar que esa etapa de la vida implica un alto grado de oposición al mundo de los adultos, pero en la que es fundamental la relación e integración con el grupo que se considera afín. Por eso no es extraño que sea una etapa donde los estereotipos de género actúan como auténticas guías de conducta individual"* (Bernárdez Rodal, 2006:80).

Lo que la autora (2006:81) ha comprobado analizando las conversaciones por chat es que, no solamente son pocos los que parecen estar interesados en cambiar su identidad sexual, sino que se esfuerzan por recurrir a los estereotipos, a las frases hechas, a todos los recursos lingüísticos que no solo "dejan ver" sino que intencionalmente se presentan a sí mismos – incluso frente a desconocidos – dejando bien en claro a qué sexo pertenecen.

"Aunque resulte descorazonador, no nos debe extrañar esta conclusión, ya que está en consonancia con los estereotipos que circulan en lo social de cómo niños y niñas deben comportarse en la adolescencia, y si algo suele atemorizar a un adolescente es sentirse diferente y extraño al grupo al que desea pertenecer" (2006:80).

9. Internet como lugar peligroso

Dejando de lado la discusión del inicio de si se trata de los "viejos dilemas" bajo nuevas formas o si existen nuevos problemas, veremos que algunos temas tienen al género como variable discriminatoria y, por ende, de vulnerabilidad diferenciada para hombres y mujeres. Vamos a destacar aquí dos de ellos: privacidad y ciberacoso.[21]

Obviamente el derecho a la vida privada vale tanto para niñas como niños. Tampoco necesariamente son diferentes las maneras en que se suele comprometer su cumplimiento; solo por nombrar algunas: el otorgamiento "voluntario" de datos personales en las re-

[21]*Cfr.* Sanz González.

des sociales, el recibimiento de correo no deseado, el tratamiento inseguro de datos sensibles (dirección, teléfono, religión, raza, historial médico, entre otros) por diversos organismos que los solicitan compulsivamente, el control exagerado de padres y tutores sobre las comunicaciones de los hijos, el seguimiento de los historiales de búsqueda por las empresas, entre otros.

Sin embargo, el tema de la privacidad como fenómeno y como preocupación, sí puede leerse en clave de género. En primer lugar porque la teoría feminista ha hecho grandes aportes a la comprensión de la distinción entre lo público y lo privado, y sus implicancias en la vida de las mujeres. En particular han mostrado cómo en las sociedades industriales de occidente ha habido una diferenciación práctica y simbólica respecto a dos ámbitos de la vida: uno, en donde se encuentran las decisiones y acciones políticas y económicas que pertenece a los hombres, y otro, relativo a la "vida privada". Dentro de este segundo ámbito, están las mujeres y los niños.

La modernidad supuso la contradicción entre la universalidad de los derechos humanos y la selectividad real de la ciudadanía. Como señala Baratta,[22] el pacto social se trató de un "*pacto ad excludendum*", por medio del cual una minoría de iguales excluyó de la ciudadanía a los diferentes: mujeres, niños, pobres, locos, etc.

La separación de lo público y lo privado, permitió la diferencia de criterios a la hora de interpretar la realidad y aplicar la ley. Bajo la sombra de que los asuntos de mujeres y de los niños eran asuntos privados, se ha incurrido en flagrantes injusticias. Se trata de una posición que encubre una cosmovisión autoritaria, ya que de la puerta para adentro el juez terminó siendo el hombre, proveedor y con el monopolio de la violencia respecto de sus hijos y su mujer, ambos considerados su propiedad.

El discurso encubridor del deber de protección del hombre, del uso de la autoridad para el bien común (la familia burguesa en total deterioro en la actualidad), de referente del saber, no ha hecho más que legitimar, conjuntamente con el Derecho moderno, la discriminación y recortar la autonomía de todo sujeto de derecho de decidir sobre su propia vida.

[22] A. Baratta, *El derecho y los chicos*, Espacio Editorial, Buenos Aires, 1995. Citado en Rozanski, 2003.

"Algunas autoras como Kramer y Kramarae,[23] resaltan que debido a que tradicionalmente las mujeres han carecido del derecho a la privacidad (empezando por no poder poseer propiedad privada) y a la autonomía en las decisiones sobre la propia vida, es mucho más difícil saber cuándo la privacidad de las mujeres está siendo violada".

Dentro de los temas que aborda el derecho a la vida privada, hay algunos que se relacionan al tradicional espacio de lo público (datos legales, fiscales, educativos, médicos, etc.) y otros que afectan a los y las ciudadanas en lo que tradicionalmente se ha encontrado en el ámbito de lo privado. Así, encontramos expresiones de gran preocupación pública frente a la exposición que tienen los niños frente a los trastornados pedófilos, pero poco se hace frente a la amplia mayoría de la violencia sexual contra los niños: la que tiene lugar en la familia y por los seres más cercanos a ellos y ellas.

También se alza la alarma pública ante la vulnerabilidad de "las chicas de bien", esas que pueden ser como su hija, que son acosadas por desconocidos en la web. ¿Cómo protegerlas en los entornos *online*? Sin embargo, parece no aplicar el derecho a la protección de la vida privada, cuando se trata de fotos y videos online, de adolescentes de "dudosa reputación", siguiendo el viejo (y religioso) principio que es la mujer la responsable por la violencia de la que es víctima.

Relacionado con la vulneración al derecho a la protección de la vida privada, pero definitivamente distinto y también con un fuerte sesgo de género, encontramos el ciber acoso.

El ciber acoso presupone una violación a la intimidad desde el momento que se utilizan en forma no consentida datos personales como el correo, el celular, el teléfono, la dirección, entre otros, pero además, en general va acompañado del abuso y daño a la imagen y a la reputación de las personas. No solo se distribuyen imágenes y audios que no fueron autorizados, sino que se violenta a una persona, se la amenaza, chantajea, se limita su libertad al incrementarle el miedo, la impotencia y la vergüenza. El ciber acosador hace un uso abusivo de su poder sobre otra persona por medio de la violencia psicológica, emocional y simbólica. A veces también física.

[23] J. Kramer y C. Kramarae, "Gendered Ethics on the Internet", en J.Makau y R. Arnett (eds.), *Communication Ethics in an Age of Diversity*, IL, University of Illinois Press, Urbana y Chicago, 1997, pp. 226-243. En Sanz González 2006:203.

Las víctimas del ciber acosador son los más débiles: mujeres, niños, minorías étnicas, "los diferentes" si la referencia es un hombre blanco occidental. Tampoco los efectos de estas vulneraciones de derecho afectan igual en los hombres que en las mujeres. Como señala Sanz González (2006:202) "*los ataques a la privacidad «informacional», además de posibilitar ataques a la integridad física de las mujeres amenazan también la «privacidad en la toma de decisiones» de éstas, en tanto que limitan sus capacidad de decidir autónomamente sobre el uso de la red para su vida privada o profesional (por ejemplo decidir si comenzar un negocio a través de Internet o concertar una cita a través de un chat)".*

También en los ciber delitos encontramos aquellos que tienen que ver con lo público y lo masculino – las estafas millonarias, las lesiones a los derechos del consumidor, el spam – y los que involucran la violación de los derechos humanos, cuyas víctimas en general son mujeres y niños, como la utilización de niños, niñas y adolescentes en pornografía.

De hecho, el cambio tecnológico ha llevado a discutir la terminología utilizada para describir el material sexualizado (imágenes, texto y archivos de audio) relacionado con niños, puesto que se presentan nuevas modalidades que, por ejemplo, cuestionan la tradicional separación entre abuso sexual infantil y explotación sexual comercial infantil. Situaciones de abuso sexual que son grabadas y luego se comercializan, a veces sin que la víctima se entere. El intercambio de fotos tal vez sensuales pero no eróticas, a cambio de una tarjeta de carga en el celular. Novios que se graban a conciencia y luego, uno de ellos o un tercero, hace un uso no consentido de ese material.

Internet permite que más material con contenido sexual se encuentre a disposición de más personas, promueve el anonimato, facilita la conexión entre sujetos con "iguales preferencias" y su intercambio de archivos. También, deja una puerta bastante más amplia abierta para el contacto directo con los niños.

Si bien las particularidades de Internet pueden ser facilitar e incluso generar tipos particulares de vulneración de derechos de mujeres, niños, niñas y adolescentes, es la reproducción de los estereotipos culturales de género lo que explica que sigan siendo éstos los grupos víctimas de la mayor parte de la violencia sexual o privada.

10. Género y violencia

Las mujeres y los niños son las mayores víctimas de violencia en la red. El ciber acoso y la pornografía son temas a ser vistos en clave de género. *"(…) refieren en última instancia al control sobre los cuerpos (femeninos e infantiles). Esto es un problema que tradicionalmente ha ejercido el género masculino sobre los cuerpos de seres que consideran «objetos de deseo» y susceptibles de ser «violados» (física o metafóricamente)",* (Sanz González, 2006:202).

La violencia atenta contra la integridad física y psicológica, contra la dignidad y contra la posibilidad de desarrollar relaciones confiables. La violencia es, en un sentido amplio, un tema político; es una "forma de hacer" en la relación entre los seres humanos. Esta forma de relacionamiento abusiva es producto de factores culturales, económicos e histórico-sociales y, en ese sentido, de la sociedad en su conjunto. La violencia sexual causa tanto rechazo que no son pocas las veces en las que se busca desesperadamente reducirla a un problema que tienen personas supuestamente "desviadas".

Los estereotipos de género también se verifican en las reacciones de las víctimas y de las instituciones que la rodean: la familia, la escuela, la comunidad, los juzgados, la policía. Así, encontramos a la niña abusada o con su reputación por el piso a causa de la difusión infinita de su imagen a través de la web, que para manejar su propia angustia idealiza a su abusador y se culpabiliza a sí misma. O padres que se sienten tan atacados que en vez de apoyar a la hija, la dejan sola, se niegan a ver qué está sucediendo en internet y, en última instancia, la culpabilizan.

La soledad y la responsabilidad de la víctima femenina no se contradicen con los estereotipos de género. Por el contrario, ideas instituidas culturalmente como la importancia de la cohesión familiar a cualquier costo, la responsabilidad de la mujer en el mantenimiento de esta cohesión familiar o la priorización de los deseos y necesidades del hombre, no hacen más que reforzar los mensajes clásicos de quien, abusando de la confianza o de su lugar de poder, violenta a la niña: "tú estabas de acuerdo y te gustaba", "tú eras mala y te lo merecías", "tú debes sacrificarte por el bien del resto de la familia" (Siegfried, Heidi en: BICE, 2002:20) y podría agregarse "tú te sacaste las fotos porque quisiste".

También en los niños varones que sufren la violencia sexual – generalmente se trata de un tipo de victimización que cesa o decae mucho en la medida en que el niño se transforma en adolescente – , las fuertes expectativas de género tienen efectos sobre las víctimas y sus entornos. El silencio en los niños se fortifica: por el miedo que el abuso provoca sobre su propia identidad sexual y el miedo a ser estigmatizado por los otros como homosexual si cuenta su historia (Siegfried Heidi en: BICE, 2002:20).

Algunas reflexiones finales

Cuando hablamos de internet es recomendable pararse desde un lugar de novedad y cambio sustancial, pero también de incertidumbre. Incertidumbre porque el determinismo tecnológico es falso e incertidumbre porque aún los procesos más generales y básicos que hoy se toman como un hecho, pueden en poco tiempo volver a cambiar. Por ejemplo las características de la web 2.0. ¿Hacia qué dirección se procesarán los cambios en internet? ¿Sabemos con certeza que la red profundizará sus cambios en la misma dirección actual? No, no lo sabemos.

Esto dependerá de grandes movimientos, tales como cuán libre será la web en un futuro cercano. Actualmente la innovación de la tecnología móvil ha abierto dudas acerca de la posibilidad de que cualquiera pueda seguir creando y subiendo contenidos libremente, al menos para ser utilizados en estos dispositivos móviles. También tendencias que parecían "imparables" como la integración de aplicaciones han demostrado no serlo tanto, si los usuarios no las aceptan. Por ejemplo se ha hecho sentir en más de una ocasión por quienes pretenden se les cuide los datos personales, que es abusivo que las compañías o los desarrolladores de software decidan conectar sus datos con nuevas prestaciones.

Es conveniente dejar a un costado posturas extremas que, o bien descontextualizan a la tecnología, o bien le quitan a los individuos sus posibilidades de acción frente a las mismas. La tecnología no llega a la humanidad de la nada ni va a modificar por sí misma sus relaciones sociales. Por otra parte, internet tiene un gran margen de variabilidad y esa variabilidad depende tanto de productores y

usuarios (individuos) como de los cambios en las fuerzas históricas, culturales, económicas y sociales que atraviesan a los individuos y a las organizaciones, los movimientos y las sociedades.

Para las mujeres, internet configura un nuevo ámbito de lucha política y social. No hemos encontrado trabajos que demuestren que internet y las TICs sean causantes explicativas de avances significativos en la efectivización de los derechos de las mujeres. Sí se ha dado cuenta de estudios que desde la teoría feminista han alimentado fuertes esperanzas respecto a las posibilidades de internet en el logro de la equidad de género. Desde la investigación empírica, más bien se han encontrado investigaciones que, desde distintas disciplinas y enfoques, llegan a conclusiones que evidencian poca diferencia en la experiencia *online* y *offline* para las mujeres.

La reproducción de los estereotipos culturales discriminatorios según género se verifica en internet, al menos en lo que hace al lugar de la mujer en la industria tecnológica y al uso que las mujeres hacemos de la web así como del tipo de experiencias que allí tenemos. Si bien siguen existiendo reivindicaciones respecto al acceso, no parece ser éste el principal factor discriminatorio.

Si entendemos internet como un espacio de socialización, comprenderemos que la reproducción en este ámbito de los patrones discriminatorios según género, impactan en la socialización de los niños y las niñas, quienes usan – cada vez más intensamente – internet como un lugar de experimentación de roles sociales.

Los y las adolescentes no parecen estar muy interesado/as en cambiar su identidad sexual en la web, aunque podrían jugar con esta posibilidad que brinda la virtualidad. Más aún, los modelos de género los orientan. Así, utilizan signos y códigos estereotipados en lo que refiere al sexo, a pesar que innovan muchísimo interviniendo en el lenguaje para generar signos y códigos que los identifiquen como grupo.

Los y las adolescentes buscan en internet principalmente un espacio propio, donde interactuar entre iguales con cierta intimidad. Los y las adolescentes, a pesar que se encuentran en un momento de definición de su identidad sexual, mayormente buscan distinguirse de los adultos y construirse en el espejo de los otros. Los modelos de género les permiten definir la situación y adoptar la fachada adecuada, siguiendo las categorías de Goffman.

Por otra parte, "liberarse" del cuerpo no es tan sencillo como tener la posibilidad de no mostrarlo. Las señales que "dejan ver" la pertenencia genérica son múltiples y se develan en la interacción con facilidad; de hecho, requerirían un enorme esfuerzo intentar conscientemente hacer invisibles estas señales.

Las posibilidades de engañar en internet también se han esgrimido como preocupación en la medida que la falsa identidad es un elemento encubridor para aquellos que utilizan internet para cometer delitos. En esta línea, es particularmente inquietante la impunidad de la que gozan por la vía de los hechos quienes se acercan a niños u adolescentes pretendiendo ser otros adolescentes.

La violencia sexual tiene un fuerte sesgo de género, puesto que la mayoría de sus víctimas son mujeres. Internet y las TICs traen consigo algunos riesgos particulares que exponen a las tradicionales víctimas de la violencia, a formas más o menos "innovadoras" de vulneraciones de derechos. Por ejemplo el ciber-acoso y la explotación en pornografía por medio del chantaje o de la utilización de imágenes sin el consentimiento de la involucrada, pone sobre la mesa el tema de la privacidad.

El asunto de la vida privada no nace con internet. Ciertamente internet plantea nuevos desafíos por sus posibilidades en la generación, publicación y transmisión de datos, pero la fuerte distinción (liberal y dicha por el hombre para asignarle un lugar a todos y a pesar de todos) entre lo público y lo privado, ha sido re leída en clave de género por la teoría feminista para criticar modelos que han buscado explicar las sociedades modernas.

El movimiento feminista y la teoría feminista, desde la praxis política, deberá seguir pensando y actuando en el espacio social de internet para auto-definirse y lograr una mayor equidad real. Lamentablemente no parece ser este un tema relevante o que motive el involucramiento activo para los y las jóvenes latinoamericanos que participan en programas de integración a la "Sociedad de la Información". Internet es una nueva arena para la lucha política.

Bibliografía

ARAÚJO, S. (2000), "As contribuiVões de Henri Wallon ao estudo do jogo no desenvolvimento da crianca e do adolescente", *Revista do Departamento de Educacao*, Universidades Católica de Goiás, Vol. 3.

BERNÁRDEZ RODAL, A. (2006), "*A la búsqueda de una 'habitación propia': comportamiento de género en el uso de Internet y los chats en la adolescencia", Revista de Estudios de la Juventud*, (73), pp. 69-82. Disponible en: http://eprints.ucm.es/10410/

BICE (2002), *Violencia Sexual contra Niñas, Niños y Adolescentes*, Oficina Internacional Católica de la Infancia, Delegación Regional para América Latina, Montevideo, Uruguay.

BONDER, G. (2008), *Juventud, Género & TIC: imaginarios en la construcción de la sociedad de la información en América Latina*, ARBOR Ciencia, Pensamiento y Cultura, CLXXXIV 733, septiembre-octubre, pp. 917-934.

BONDER, G. (2001), "Las nuevas tecnologías de información y las mujeres: reflexiones necesarias", (Versión preliminar). Documento para participantes de la Reunión de Expertos sobre Globalización, Cambio Tecnológico y Equidad de Género, llevada a cabo en Sao Paulo, Brasil, 5 y 6 de noviembre de 2001, por CEPAL, Universidad de San Paulo, Conselho Nacional dos Direitos de la Mulher, UNIFEM y GTZ.

BUTLER, J. (1990), *Gender Trouble: Feminism and the Subversion of Identity*, New York, Rouledge.

CASAS, F. (1998), *Infancia: perspectivas psicosociales*, Paidós, Barcelona, España.

CASTELLS, M. (2001), *La galaxia internet*, Plaza y Janes, Barcelona, España.

—— (2001), *Internet y Sociedad Red*, Programa de doctorado sobre la sociedad de la información y el conocimiento (UOC), disponible en: http://www.uoc.edu/web/cat/articles/castells/castellsmain2.html

ECPAT International (2008), "Child Abuse Images and Sexual Exploitation of Children Online". Preparatory Expert Meeting for the World Congress III against Sexual Exploitation of Children and Adolescents. Bangkok, Thailand. Disponible en: http://www.ecpat.net/WorldCongressIII/PDF/Publications/ICT_meeting_Report.pdf

—— (2009), "Child Pornography and Sexual Exploitation of Children Online". Disponible en: http://www.ecpat.net/EI/Publications/ICT/Child%20Friendly_Child%20Pornography_FINAL.pdf

FALLOWS, D. (2005), "How Women and Men Use the Internet", *Pew Internet and American Life Project*. Disponible en: http://www.pewinternet.org/Reports/2005/How-Woman-and-Men-Use-the-Internet.aspx

FOUCAULT, M. (1992), *Microfísica del Poder,* Editorial La Piqueta, Madrid, España.

GEERTZ, C. (1997), *La interpretación de las culturas*, Gedisa, Barcelona, España.

GOFFMAN, E. (1959), *The Presentation of Self in Everyday Life*, Doubleday Anchor, New York.

HERRERA GÓMEZ, M. y R. M. SORIANO MIRAS (2004), "La teoría de la acción social en Erving Goffman", *Papers: Revista de Sociología*, Núm. 73, pp. 59-79.

LEMINEUR (2006), *El combate contra la pornografía infantil en Internet: el caso de Costa Rica*, OIT/IPEC, San José, Costa Rica.

MARTIN-BARBERO, J. (2000), *Culturas/Tecnicidades/Comunicación, Iberoamérica: Unidad Cultural en la Diversidad*, OEI. Disponible en: http://www.oei.es/cultura2/barbero.htm

MILLER, H. (1995), *The Presentation of Self in Electronic Life: Goffman on the Internet*, Department of Social Sciences, The Nottingham Trent University. Presentado en Embodied Knowledge and Virtual Space Conference, Goldsmiths College, University of London, Junio.

PISCITELLI, A. (2006), *Nativos e inmigrantes digitales. ¿Brecha digital, brecha cognitiva o las dos juntas y aún más?*, RMIE, Vol. 11, N° 28, pp.179-185. Disponible en: http://www.scribd.com/doc/467656/Nativos-e-Inmigrantes-Digitales

PLAN, S. (1998), *Zeros and ones: Digital women and the new techno culture,* Fourth Estate, London.

PRENSKY, M. (2001), *Digital Natives, Digital Inmigrants*, MCB University Press, Vol. 9, N° 5. Disponible en: http://www.marcprenski.com/writing/

QUAYLE, LOOF, PALMER (2008), *El uso de niños, niñas y adolescentes en pornografía y la explotación sexual de menores en Internet*, Jaap Doek (Editor de la Serie). Presentado por ECPAT International en el III Congreso Mundial contra la ESNNA. Disponible en: http://www.ecpat.net/WorldCongressIII/PDF/Publications/ICT_Psychosocial/Thematic_Paper_ICTPsy_SPA.pdf

ROZANSKI, C.A. (2003), *Abuso Sexual Infantil, ¿Denunciar o Silenciar?*, Ed. B. Argentina S.A., Buenos Aires.

SANZ GONZÁLEZ, V. (2006), "Las tecnologías de la información desde el punto de vista de género: posturas y propuestas desde el feminismo", Instituto de Filosofía, CSIC, ISEGRORÍA, Nº 34, Madrid, España, pp. 193-208.

SAZ RUBIRA, J.M. (2004), *Aplicación educativa de los videojuegos*, Educar en el 2000, abril, 2004.

WAJCMAN, J. (2004), *Technofeminism,* Polity Press, Cambridge, Reino Unido.

WINNICOTT, D. (1990), *Realidad y Juego*, Gedisa, Buenos Aires.

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 digitales 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.

"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.

[1]Véase 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

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

[2]Cabe 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

[3]*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

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]

[4]Este 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 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 vinculo electrónico siguiente: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0375:ES:HTML

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.

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

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

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-

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

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

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 victimas 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 deshonroso 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 gobierno de las bases de datos, de perfiles y de técnicas de autorización de seguridad.

[9]La 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.

[10]De 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/

[11]Michael 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.

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]

[12]Véase 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

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

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

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

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. Poullet, "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.

[15]Disponible para su consulta en el vinculo electrónico siguiente: http://www.informatica-juridica.com/anexos/anexo476.asp

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

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

[18]Y. Poullet, "Hacia nuevos principios… *Op.cit.*, p. 37. [Énfasis añadido].

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 legitima 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:

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

[20]En 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

[21]En particular consultar la "Recomendación" 3/97… *Op.cit.*, p.7.

- 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, vinculo 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

[22]En 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.

[23]A 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.umlaw.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

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

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

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 3/97[25]

- 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] *Ibíd.*, p. 13

- Los medios anónimos de acceso a Internet (p. ej., kioskos 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 intimo balance con el derecho a la libertad de expresión.

[26] Los "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 finalidad 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/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

[27] "Recomendación 3/97… *Op. cit.*, p. 13.

[28] *Ídem*.

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

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

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 distribuyo panfletos afuera de la

[30]En 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.

[31]Por 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*.

Blendon Middle School en Westernvill, 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 dlls., 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]

[32]A 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).

[34]A 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*.

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, accesar 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-deadthof.pdf

[35]El 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.europea.eu/justice_home/fsj/privacy/index_en.htm

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 una 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.

[36]En 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.

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 riegos 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]

[37]Para más información sobre la labor de las Agencias de Protección de Datos en el mundo, puede consultarse la página oficinal 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.privacyconference2009.org/

[38]Milton 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.

[39]El 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 res social de la persona o la organización a quien se calumnia o descalifica. Específicamente, a través de tecnologías de carácter

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.

[40]Véase 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.

DECALOGO DE DERECHOS DE LAS NIÑAS, NIÑOS Y ADOLESCENTES EN LAS TIC[41]

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.

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

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 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.

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

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

[43]Véase, *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

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 explicito que los

[44]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 Parlamentaria*, Número 21, Año 2006. Disponible en el vínculo: http://www.senado.gob.mx/sgsp/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*.

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

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.

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

—— (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

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.europea.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

"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/portalwebAGPD/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/

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

Resolución sobre Protección de la Privacidad en los servicios de redes 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 explotación 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 Parlamentaria, 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 Internet*. 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 Oxford sobre la Protección de la Infancia y la Libertad de Expresión en Línea (2010). Disponible en formato digital en el vínculo: http://www.oii.ox.ac.uk/news/?id=405

Redes sociales y vida privada: una ecuación posible

Rosario Duaso Calés[*]

1. Nuevas modalidades de vigilancia y múltiples riesgos de vulneración del derecho a la vida privada

Es interesante observar cómo los riesgos para la protección de los datos personales se manifiestan en la actualidad de manera muy importante en el ámbito de las relaciones "sociales" que se desarrollan *online*. Efectivamente, las relaciones que se establecen gracias a las redes sociales en Internet, tienen como consecuencia inmediata la revelación de los detalles de dicha relación y la persistencia de dichas informaciones en la red de forma permanente. El ser muy "sociable" en la red conlleva la revelación de todos los aspectos de la personalidad de los usuarios y a veces, de terceros que ni siquiera han consentido a que sus datos se encuentren disponibles en este contexto.

Normalmente estas relaciones tienen como base la voluntad de las personas implicadas en las mismas, ya que la red social es utilizada por aquellos que quieren que esta plataforma sirva de me-

[*]Investigadora en el equipo de derecho relativo a las tecnologías de la información y de la comunicación del *Centre de recherche en droit public* de la Universidad de Montréal, Canadá.

dio para comunicar con todos aquellos que también formen parte de dicha comunidad. La cuestión es compleja ya que el usuario de la red social no siempre es consciente de los riesgos a los que se enfrenta al "virtualizar" unas relaciones sociales que cambian significativamente su naturaleza como consecuencia del medio que las sustenta: Internet.

La tecnología empleada y más concretamente, las modalidades de utilización que cada red social establece, intensifica o disminuye directamente el nivel de riesgos relativos a la confidencialidad de lo que sucede en la relación social.

Lo que es privado o público se difumina en ocasiones y lo que creemos que es compartido por un número muy reducido de amigos puede ser difundido a un número incalculable de personas durante un tiempo indefinido y de forma peligrosamente descontextualizada. Algunos autores aportan términos interesantes que simbolizan la complejidad de lo que implica el uso de las redes sociales, ya que podemos hablar de las nociones de lo "públicamente privado" y de lo "confidencialmente público"[1] para representar la confusión que impera en la actualidad y sus consecuencias jurídicas.

El papel de la industria para establecer los parámetros de privacidad que permitan proteger los datos personales de usuarios y terceros es de vital importancia y determina en gran medida cómo cada uno de los usuarios va a protegerse de los riesgos concretos.

El acceso no autorizado y a veces autorizado a los datos por parte de terceros puede tener consecuencias perjudiciales tanto en la esfera privada como en la esfera profesional y puede desvelar aspectos de la vida íntima que pueden causar graves perjuicios a los titulares de los datos.

Es difícil identificar a todos aquellos que puedan estar interesados en conocer la gran cantidad de información que es almacenada en las páginas personales de los usuarios y esto es así porque en realidad la información está allí para todo aquel que pueda necesitarla en cualquier momento y para ser utilizada para cualquier finalidad.

[1]Miyase Christensen, 'Facebook is watching you', *Le Monde diplomatique*, en Manière de voir, Internet, révolution culturelle, 109, febrero-marzo 2010, pp. 52-55. (Traducción libre de la versión original en francés).

Es muy interesante la reflexión sobre cómo si en los años 1980 el peligro de la sociedad de la información estaba representado por el *"Big Brother"*, la época actual caracterizada por las redes sociales, se puede considerar como "la encarnación de un deseo latente de una mirada bienintencionada y fraternal (del tipo *hermano a hermano*) o incluso como un acto inocente de "voyeurismo amistoso".[2]

En efecto, se produce un cambio significativo que incide claramente en quién accede a la información difundida en una página personal y cómo se produce dicho acceso. Esta nueva forma de vigilancia provoca une reevaluación de los peligros por parte del usuario si bien, el riesgo de vigilancia procede también del sector público y privado, por lo que el riesgo puede presentarse más complejo, difuso e incontrolado que en el pasado.

El papel del usuario es vital para gestionar la protección de sus informaciones, pero para ello es necesario que se encuentre informado de los riesgos que su participación en una red social conlleva y de los mecanismos de los que realmente se dispone para hacer efectiva la protección deseada.

Lo novedoso es también la llegada de profesionales especializados que S. Baker ha denominado *numerati* y que trabajan en "encontrar patrones significativos entre las cada vez mayores montañas de datos digitales".[3] Son ingenieros, matemáticos e informáticos que van a procesar la información que cada uno de nosotros dejamos en Internet y en la utilización cotidiana de diferentes tecnologías que están a nuestro alcance, comparando estos datos con otros de los que disponen, con el objetivo de conocer todos los aspectos inimaginables del comportamiento humano.

Esto no hace más que ilustrar nuevas modalidades de vigilancia, pero también, tal y cómo nos explica este autor, la existencia de una línea divisoria en nuestras sociedades: "hay un foso divisorio entre aquellos que quieren que las máquinas estén informadas y sean inteligentes y los que prefieren que se queden en la oscuridad. Así que la línea divisoria sobre privacidad no es entre los *numerati* y el resto de la humanidad; existe (y se hace cada vez más ancha) entre

[2]*Ibid.*, p. 54. (Traducción libre de la versión original en francés).

[3]Stephen Baker, 'Nos vigilan', *El País Semanal*, nº 1.730, 22 de noviembre de 2009, pp. 58-63.

las personas que tienen diferente opinión sobre ese tratamiento de la acumulación de datos personales".[4]

En efecto, nos encontramos en una época en la que resulta importante posicionarse respecto al "yo virtual" que cada unos de nosotros desea mostrar, ya que las implicaciones de lo que somos en la red tiene consecuencias importantes a la hora de lograr una protección efectiva de nuestro derecho a la intimidad.

2. Reacciones globales para lograr la efectividad del derecho a la protección de los datos personales en el contexto de las redes sociales

Podemos afirmar que la cuestión de los riesgos relativos a la protección de los datos personales en las redes sociales existentes en Internet representa una problemática jurídica que despierta inquietudes desde hace algunos años.

El derecho a la vida privada de los utilizadores y de terceras personas se puede ver afectado, ya que un elevadísimo volumen de informaciones de todo tipo, fotos y videos se encuentra disponible en línea.

Cuando el utilizador es un menor de edad, esta cuestión se agrava ya que los riesgos se multiplican y se amplifican considerablemente, siendo nefastas las consecuencias de la vulneración del derecho a la protección de sus datos de carácter personal. Son muchos los que denuncian los peligros que estas plataformas engendran especialmente para los niños y adolescentes, grupo especialmente vulnerable muy activo en las diferentes redes sociales y muy a menudo víctimas de acoso, de chantajes, de suplantación de identidad y de utilización ilegítima de sus datos personales.[5]

Identificamos igualmente riesgos derivados de la gran masa de informaciones sobre el comportamiento de los usuarios de estas redes sociales de las que se puede disponer para fines diversos. La

[4] *Ibid*., p. 61.

[5] Olivier Levard y Delphine Soulas, *Facebook: mes amis, mes amours… des emmerdes!, La verité sur les réseaux sociaux*, Paris, Michalon, 2010, pp. 67 y ss.

gratuidad de estas redes va acompañada de una publicidad dirigida a los usuarios que podemos calificar de "personalizada" y que responde a un perfil muy concreto que se obtiene a partir de las informaciones publicadas en las páginas personales. Si bien la publicidad que es realizada por ciertos motores de búsqueda se realiza a partir de las búsquedas que cada utilizador realiza, la publicidad proveniente de estas redes deriva de forma directa de lo que publicamos sobre nosotros y por lo tanto, de nuestro "yo" más íntimo.[6]

La cuestión de quién puede acceder a las informaciones que cada usuario pone en línea es fundamental, ya que el acceso por parte de terceros a los diferentes datos puede llevar a utilizaciones abusivas de los mismos. El resultado de esta pérdida de control que cada uno cree ejercer sobre sus datos revela la gran vulnerabilidad de los usuarios de las redes sociales y da lugar al quebrantamiento de los más básicos principios de protección de datos y muy especialmente, del principio de finalidad.

No podemos negar que las redes sociales se han convertido en una verdadera mina de información muy útil para entidades del sector público y privado que pueden servirse de las mismas para obtener datos que los utilizadores en ningún caso han pensado que pudieran ser accesibles a terceros.

El respeto de las leyes de protección de datos personales por parte de la industria de las redes sociales plantea problemas que derivan muy directamente de la complejidad que rodea a este fenómeno. En efecto, cada red social opera a nivel mundial y tiene vocación de servir de plataforma de comunicación para el mayor número de usuarios en el mundo. Sin embargo, cada red social debe respetar la legislación de protección de datos de cada país en el que opera, ya que cada usuario debe gozar de la protección que sus leyes nacionales le ofrecen.

Resulta evidente que una respuesta global al problema del respeto de la privacidad en el ámbito de las redes sociales es necesaria, ya que es únicamente esta la que puede tener un impacto para lograr un equilibrio entre los intereses de la industria y el respeto del derecho a la vida privada de usuarios y terceras personas.

[6] Jerôme Bouteiller, Claire Germouty y Karine Papillaud, *Bienvenue sur Facebook, Le mode d'emploi*, Paris, Albin Michel, 2008, p. 128.

En 2008 las Autoridades de Protección de Datos y Privacidad adoptaron una Resolución sobre Protección de la privacidad en los servicios de redes sociales,[7] lo cual demuestra la importancia que todas ellas atribuyen a esta cuestión y la voluntad de neutralizar los riesgos que estas redes generan en lo que se refiere a la protección de la vida privada. Dichas Recomendaciones están destinadas a los usuarios de las redes sociales, comportan una serie de puntos esenciales y contienen un llamamiento a proveedores de servicios, gobiernos y organismos para la protección de datos, para que realicen una labor educativa con los usuarios, dirigida a proteger sus informaciones y a hacerles llegar el contenido de dichas recomendaciones.

Este tipo de mensaje es fundamental y muy necesario en un contexto en el que algunos países que cuentan con legislación en materia de protección de datos encuentran dificultades para que las redes sociales respeten sus preceptos y otros muchos países ni siquiera han legislado, no pudiendo ofrecer una protección a los usuarios frente a este fenómeno.

3. Una acción concreta para lograr que la industria respete los principios sobre protección de datos

La Oficina del Comisionado de la Privacidad de Canadá (*Office of the Privacy Commissioner of Canada*), tiene por misión la defensa del derecho a la protección de la vida privada de los canadienses. La posición de esta autoridad de protección de datos en el contexto de las redes sociales supone un ejemplo de efectividad de las medidas adoptadas para lograr que la red social *Facebook* respete los principios esenciales de la protección de datos que las leyes canadienses en la materia recogen.

[7] *Resolución sobre Protección de la privacidad en los servicios de redes sociales*, adoptada en la 30 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Estrasburgo, 17 de octubre de 2008. Disponible en el vínculo siguiente: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/08-10-17_Strasbourg_social_network_ES.pdf

3.1 La posición del Comisionado de Privacidad de Canadá en su investigación sobre *Facebook*

En mayo de 2008 se deposita ante la Oficina del Comisionado de la Privacidad de Canadá una denuncia por parte de la *Canadian Internet Policy and Public Interest Clinic*, sobre un conjunto de prácticas y políticas en materia de protección de datos personales llevadas a cabo por la red social *Facebook*.

Esto desencadena una investigación llevada a cabo en virtud de la ley federal canadiense en materia de protección de datos de carácter personal que se aplica al sector privado en Canadá, la PIPEDA o *Personal Information Protection and Electronic Documents Act*.[8]

Un año más tarde, en julio de 2009 se publica un Informe de conclusiones sobre el dossier abierto sobre *Facebook*, que anunciaba el final de dicha investigación y que desvela que de la misma derivaban varias preocupaciones relativas a la protección de la privacidad en esta red social, si bien alguna de ellas no se había podido resolver con éxito.

Más concretamente, dicho Informe establecía que cuatro aspectos de la denuncia estaban fundados y otros cuatro estaban fundados y considerados como resueltos al haber *Facebook* aportado los cambios necesarios para ello a sus políticas y prácticas en materia de privacidad. Sin embargo, otros cuatros aspectos de la denuncia habían sido rechazados por no estar fundamentados jurídicamente.

Quedaban por lo tanto, cuatro aspectos de la denuncia fundados y a la espera de una resolución. Dichos aspectos que hacían referencia a temas como la protección de los datos de los no-usuarios de la red social o las condiciones de la desactivación de las cuentas debían ser tomados en cuenta por *Facebook* si la red social quería respetar la legalidad en Canadá.

Es importante tener en cuenta que en 2010 *Facebook* contaba ya con más de 550 millones de usuarios activos en el mundo, lo que hace de esta plataforma la red social más importante del mundo en cuanto al número de usuarios, sin olvidar que casi la mitad de los

[8] L.C. 2000, ch. 5.

canadienses están inscritos en *Facebook*.[9] Resulta llamativo igualmente saber que Canadá es junto con Brasil los dos países más "conectados socialmente" del mundo.[10]

En este Informe de julio 2009 la Oficina del Comisionado de la Privacidad de Canadá da un plazo de 30 días a *Facebook* para conformarse a las recomendaciones que quedaban pendientes por resolver. Durante este periodo ambos continuarían trabajando juntos para llegar a una solución a las preocupaciones expresadas por el Comisionado. Si en este plazo de 30 días la red social no atendía a las peticiones y recomendaciones concretas, modificando en su sistema todo aquello que pudiera vulnerar el derecho a la vida privada de millones de canadienses, el Comisionado llevaría a *Facebook* ante la Corte Federal de Canadá (*Federal Court of Canada*).

En virtud del *Personal Information Protection and Electronic Documents Act*, la Oficina del Comisionado de la Privacidad de Canadá puede acudir a la Corte Federal Canadiense para forzar la adopción de la medidas de modo a lograr la conformidad con esta ley canadiense.

Si en cierto modo la actuación de la Oficina del Comisionado de la Privacidad de Canadá nos resulta de una importancia particular es porque en su momento, supo buscar una verdadera conformidad de las políticas de privacidad de *Facebook* con la legislación canadiense en la materia.

Para ello se sirvió de los recursos que la ley le confiere para lograr el respeto del derecho a la vida privada en Canadá y desencadenó los procedimientos existentes para que la industria se confrontara a la verdadera cuestión que a nuestro parecer, es el respeto de los principios básicos de protección de datos.

Tal y como se ha recordado, la Oficina del Comisionado planteó un "ultimátum a *Facebook*", lo cual sirvió para recordar a la red social el riesgo que corría al no respetar las legislaciones nacionales en materia de protección de los datos personales y también

[9] *Office of the Privacy Commissioner of Canada*, "La vie privée à l'ère du réseautage social: Les obligations légales des sites de réseautage social". Discurso pronunciado por la Comisionada Jennifer Stoddart, en la Universidad de Saskatchewan, 22 de noviembre de 2010, http://www.priv.gc.ca/speech/2010/sp-d_20101122_f.cfm

[10] Olivier Levard, Delphine Soulas, *Op. cit.*, p. 32.

como detonante para que otras autoridades de protección de datos reforzaran su presión sobre *Facebook* y sobre las redes sociales en general.[11]

La posición canadiense tiene una particularidad que es digna de ser resaltada y esta es, el ejercer una verdadera presión frente a la industria, haciendo público el hecho de que *Facebook* no estaba respetando los principios esenciales de las leyes canadienses en materia de privacidad.

La prueba del efecto inmediato de dicha presión fue el anuncio un mes más tarde, en agosto de 2009, de la respuesta positiva por parte de *Facebook* en cuanto a las exigencias de la Oficina del Comisionado canadiense. El Comisionado pudo entonces anunciar que la red social se comprometía así a realizar los cambios necesarios para responder así a las cuestiones relativas a la protección de la privacidad que todavía no habían sido solucionadas.

Los cambios a los que *Facebook* se comprometía debían ser realizados en un periodo no superior a un año, durante el cual, el Comisionado podría seguir de cerca los "progresos realizados" por parte de la red social con el objetivo de lograr la conformidad con la normativa canadiense.[12]

Un año más tarde, en septiembre de 2010, la Comisionada anunciaba que el examen de las modificaciones realizadas por *Facebook* había terminado y afirmaba que todos los elementos que se habían identificado y que debían ser objeto de modificación habían sido resueltos de forma satisfactoria. Se ponía así punto final a esta investigación y se apuntaba que se habían conseguido varios cambios significativos que respondían plenamente a la ley canadiense.

Se logró por lo tanto, que la red social al realizar las modificaciones pertinentes en su sistema, respetara plenamente los principios básicos de protección de datos que establecen las reglas esenciales aplicables al tratamiento, comunicación, conservación y gestión en general de los datos personales de modo a protegerlos de forma efectiva.

[11] Esther Mitjans i Perelló, 'Ultimátum a Facebook', *La Vanguardia*, jueves 13 de agosto de 2009.

[12] *Office of the Privacy Commissioner of Canada*, "Fiche documentaire: Le suivi de l'enquête sur Facebook est terminé", 22 de septiembre de 2010. Disponible en el vínculo siguiente: http://www.privcom.gc.ca/media/nr-c/2010/bg_100922_f.cfm

3.2 Elementos fundamentales de la investigación para lograr la conformidad con las leyes de protección de datos

La red social tomó varias medidas fundamentalmente orientadas a limitar la comunicación de los datos personales a terceras empresas que desarrollan las distintas aplicaciones y juegos que son accesibles a través de *Facebook* para los usuarios. Podemos identificar igualmente otras medidas que tenían como objetivo el que la red social pudiera ofrecer una información mucho más precisa y transparente sobre cómo se gestionan los datos de usuarios y de terceras personas.

Leyendo los documentos relativos a esta investigación, comprendemos la complejidad de la misma, derivada en muchos casos de la complicación que supone que las redes sociales estén en constante evolución, y que concretamente la red *Facebook* haya cambiado mucho en los últimos años, lo cual demuestra la necesidad de examinar de forma permanente sus prácticas relativas a la protección de la vida privada.

En este caso concreto, la investigación sirvió para identificar muchas de las inquietudes relativas a la protección de la privacidad en el contexto de las redes sociales. Pero la investigación se centró en ocho cuestiones principales que preocupaban particularmente al Comisariado. Sin embargo, tal y como hemos mencionado con anterioridad, dos grandes temas han supuesto los elementos centrales que han determinado cómo se produjeron las duras negociaciones con la red social para lograr un mayor nivel de confidencialidad de los datos personales.

El primero hacía referencia a una enorme preocupación contenida en la denuncia y que era relativa al acceso casi ilimitado que terceros, como las empresas que desarrollan juegos y demás aplicaciones que se ofrecen en la red social, tenían a los datos de los usuarios.

Esta cuestión era compleja y preocupó mucho a la Comisionada, por el hecho de que existe una gran cantidad de terceros en el mundo entero que desarrollan las múltiples aplicaciones que se ofrecen en la plataforma. Se temía por lo tanto, que *Facebook* no pudiera evitar desde el punto de vista técnico el acceso de todos estos terceros a los datos personales de los usuarios y de sus amigos en la red social.

Finalmente, un sistema basado en una solución técnica permite establecer un modelo que descansa en autorizaciones mediante un consentimiento explícito para cada categoría de datos personales a los que se quiera acceder. Tal y como el Comisionado ha declarado, esto supone un gran avance ya que, se informa al usuario de las categorías de datos a los cuales se necesita acceder para que una aplicación funcione y en función de esto se pide una autorización específica y se consiente a un acceso muy controlado a un número limitado de datos.

En efecto, esta solución técnica ayuda al respeto del principio básico de no comunicación de los datos personales y la obligación legal de prestar el consentimiento por parte del titular para que terceros puedan conocer y utilizar sus datos personales.

Por otro lado, se demuestra claramente la gran importancia que adquiere hoy en día el principio de *Privacy by Design* o privacidad por diseño, basado en que el propio diseño de la tecnología sea protector de la privacidad, logrando con ello contar con arquitecturas de sistemas basadas en el respeto del derecho a la vida privada. Si este principio es respetado desde el momento de la concepción de los sistemas, se pueden evitar vulneraciones del derecho a la protección de datos y se garantiza más fácilmente el respeto a las diferentes leyes en la materia que están en vigor en los diferentes países.

Nos parece importante el mencionar la adopción en 2010 de la Resolución[13] sobre el principio de *Privacy by Design*, aprobada por la totalidad de las autoridades de protección de datos a nivel mundial, lo cual simboliza la importancia que este principio y lo que su respeto puede representar en la carrera por conseguir que el uso de las nuevas tecnologías no sea sinónimo de vulneración del derecho a la vida privada.

Cabe señalar igualmente cómo en el contexto del proceso de revisión del marco europeo de protección de datos, se alzan voces[14] apoyando la idea de que este principio de *Privacy by Design* forme parte de la nueva legislación en la materia.

[13] *Privacy by Design Resolution*, 32nd International Privacy of Data Protection and Privacy Commissioners, 27-29 de octubre de 2010, Jerusalen, Israel. Disponible en el vínculo siguiente: www. privacybydesign.ca

[14] *Controlador Europeo de Protección de Datos*, "Opinion of the European Data

Las redes sociales no deben ni pueden ignorar la gran importancia de este principio que sin duda puede ser determinante en que estas plataformas sean respetuosas con la confidencialidad de los millones de datos de los que disponen sobre un elevadísimo número de personas.

El otro tema de gran importancia que esta investigación vino a subrayar hacía referencia a la ausencia de un nivel adecuado de transparencia sobre cómo se establecían los parámetros de privacidad en la plataforma, lo cual llevaba a un gran desconocimiento por parte de los usuarios. En consecuencia, *Facebook* ha realizado cambios importantes con el objetivo de que sus prácticas sean más respetuosas con la legislación canadiense sobre privacidad.

Se consiguió entre otras cosas, que los cambios permitieran que cada usuario eligiera el grado de protección que quería acordar a sus datos personales entre tres niveles de protección o explicar claramente a los nuevos usuarios cuáles son los parámetros de privacidad de la plataforma. Se ha conseguido por lo tanto que estos parámetros se "simplifiquen" de manera significativa, ya que se puso en funcionamiento un mecanismo técnico que permite a los usuarios que acuerden un parámetro de confidencialidad concreto para cada foto, comentario o cualquier otro material, logrando con ello un mayor control por parte de cada usuario sobre sus propios datos.

Se quería por lo tanto conseguir el establecimiento de estos parámetros de privacidad "por defecto",[15] logrando así un mayor nivel de protección de los datos personales de los usuarios de la red social.

Estos no han sido los únicos cambios que han mejorado la protección de la privacidad en *Facebook* tras dicha investigación, pudiendo mencionar igualmente aspectos para facilitar la supresión o desactivación de una cuenta, cuestiones relativas a las cuentas de los

Protection Supervisor on the Communication from the Commission to the European Parliament". *The Council, the Economic and Social Committee and the Committee of the Regions – A comprehensive approach on personal data protection in the European Union*, 14 de enero de 2011, p.23. Disponible en el vínculo siguiente: www.edps.europa.eu

[15] *Office of the Privacy Commissioner of Canada*, "Fiche documentaire: Le suivi de l'enquête sur Facebook est terminé", 22 de septiembre de 2010. Disponible en el vínculo siguiente: http://www.privcom.gc.ca/media/nr-c/2010/bg_100922_f.cfm

usuarios fallecidos o incluso sobre la información que debe ofrecerse en las condiciones de utilización de la plataforma en lo que respecta a la protección de la confidencialidad de los datos personales de terceras personas que no son usuarios.[16]

El Comisionado canadiense, una vez dada por finalizada dicha investigación, no ha dejado de observar cómo esta red social trata el tema de la protección de datos de millones de canadienses.

En los últimos tiempos, el Comisionado ha recibido múltiples denuncias sobre aspectos relativos al respeto del derecho a la privacidad por parte de la red social *Facebook*, que no estaban contenidos en el marco de la primera investigación. Será muy interesante el observar cómo se gestiona en el futuro el seguimiento de estas denuncias y ver si efectivamente se puede continuar buscando compromisos con la industria en esta materia, mediante negociaciones que tal y como hemos visto, pueden dar frutos muy importantes.

Algo que se señala desde el Comisionado es que se ha conseguido que *Facebook* realizara cambios que van a servir para proteger el derecho a la vida privada de utilizadores de todo el mundo. Efectivamente la posición que se ha adoptado en Canadá ha contribuido a que la plataforma haya tomado medidas que van a repercutir en la defensa del derecho a la protección de datos personales a nivel mundial y esto es realmente un logro que demuestra el impacto que ha podido tener este asunto más allá de las fronteras canadienses.[17]

Sin dudad alguna, la posibilidad de acudir a la Corte Federal Canadiense en el plazo de un mes tuvo el impacto esperado y sirvió para ejercer una presión sobre *Facebook*, desencadenando unas negociaciones de las que han nacido compromisos importantes.

[16] Para conocer más en detalle todo lo relativo a esta investigación, se puede consultar el siguiente informe: *PIPEDA Case Summary #2009-008, Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act*. Disponible en el vínculo siguiente: http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

[17] *Office of the Privacy Commissioner of Canada*, "Communiqué: La Commissaire à la protection de la vie privée termine son examen de Facebook", Ottawa, 22 de septiembre de 2010. Disponible en el vínculo siguiente: http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_f.cfm

La presencia de nuevos riesgos para la protección de la vida privada, demuestra la importancia de llevar a cabo acciones concretas en defensa de la aplicación de los principios básicos de protección de datos.

Los millones de usuarios de redes sociales deben adoptar las precauciones necesarias para que los datos que desean mantener de forma confidencial no puedan ser el objeto de utilizaciones no autorizadas para lo cual, es vital que se puedan conocer los riesgos que la participación en dichas redes puede presentar.

La transparencia sobre cómo se gestionan los datos de los usuarios es vital y los parámetros de confidencialidad que las redes sociales ofrecen a sus usuarios deben ser respetuosos con las leyes de protección de datos y muy especialmente en lo concerniente al principio del control que todo titular debe poder ejercer sobre sus propios datos.

Las respuestas globales al fenómeno mundial de las redes sociales con el objetivo de crear un marco protector de la privacidad son necesarias para hacer llegar el mensaje a todos los actores implicados. Las acciones concretas que puedan llevar a que la industria adopte los principios de protección de datos en sus diferentes aplicaciones y en la estructura misma de las redes sociales pueden ayudar a materializar la difícil ecuación entre vida privada y redes sociales.

Protección de la privacidad y datos personales de niños, niñas y adolescentes en la web: *una responsabilidad compartida*. La experiencia educativa en Cundinamarca, Colombia

Walter Esquivel Gutiérrez y Zareth Díaz García[*]

"Se debe promover una política educativa –expresada en términos acordes a la edad de las niñas, niños y adolescentes– que incluya una estrategia informativa y formativa que les ayude a gestionar las potencialidades y los riesgos derivados de la Sociedad de la Información y el Conocimiento, en especial del uso de Internet y de las redes sociales digitales".
Memorándum de Montevideo, 2009

A manera de encuadre

...Computadoras, *software*, celulares, internet, navegar, ciberespacio, nativos y migrantes digitales, comunicación mediada por computadora, redes sociales, wikis, chats, foros, blogs y fotologs, teletrabajo, e-justicia, comercio electrónico, e-privacidad, identidad digital, ciberseguridad, e-gobernanza, empoderamiento digital, ciberciudadanía...

[*]Walter Esquivel Gutiérrez es evaluador, investigador, consultor y gestor de proyectos sociales. Por su parte Zareth Díaz García es docente, investigadora y consultora pedagógica.

Actualmente estos conceptos y otros miles relacionados, se están convirtiendo en parte integral de un vocabulario colectivo y de un imaginario social en acelerado proceso de crecimiento. Surge entonces como interrogante, conocer cómo estas expresiones de la Sociedad de la Información y el Conocimiento (SIC) están siendo comprendidas e incorporadas por los distintos actores sociales, principalmente porque dichos productos culturales están presentes en todos los ámbitos del quehacer humano, transformado desde las estrategias de socialización y construcción de identidad, hasta las formas de movilización social y generación de riqueza.

Un abordaje centrado en niñez y adolescencia sobre este tema, reconoce como el acelerado desarrollo tecnológico que caracteriza la SIC, permite a las nuevas generaciones el acceso a "...una amplia gama de oportunidades –comunicación, desarrollo de la identidad, participación ciudadana, aprendizaje, educación e inserción en el mundo productivo–, pero también de riesgos --tipos de contenido asociados con la explotación sexual comercial y no comercial; la apología de la violencia como medio para resolver conflictos; el racismo y la homofobia; la amenaza a la privacidad o a la propiedad; y la exposición a una comercialización indiscriminada" (Livingston, 2003 citado por Paniamor/IIP-UCR/SCS 2008).

Realidad que propicia un amplio espectro de oportunidades para el desarrollo personal y social de esta población, empero, dependiendo de la calidad del uso que se haga de estas herramientas, también ofrece condiciones propicias para la vulneración de derechos fundamentales, lo que no ha sido posible contener en su totalidad por la jurisprudencia tradicional, debido a que estos nuevos desarrollos avanzan a un ritmo de crecimiento vertiginoso en comparación con la legislación nacional y transnacional de protección, lo que en consecuencia ha dejado espacios sin definición de derechos, o definidos por la lógica del mercado, que en la mayor parte de los casos, es opuesta a los Derechos Humanos.

En este sentido, la vulneración de los derechos de poblaciones sujetas a mecanismos de protección especial –como lo son niños, niñas y adolescentes (NNA)– en el contexto del movimiento social en Internet, está asociado a la coexistencia de conductas y factores de riesgo (Paniamor/IIJusticia/SCS, 2009), que confluyen en la generación de escenarios de vulneración de derechos asociados en el primer caso, a la calidad de sus prácticas de interacción en la web;

y en el segundo, a la falta de políticas públicas y legislación de protección para NNA en ámbitos virtuales de carácter transnacional; la aún limitada participación del sector empresarial de Tecnologías de Información y Comunicación (TIC) en la implementación de estrategias de comercialización con enfoque de Responsabilidad Social; y el carente o nulo acompañamiento adulto desde el hogar y la escuela, esto último asociado a la falta de conocimiento de las nuevas tecnologías, comúnmente referida como Brecha Digital Generacional.

Ante lo cual, como lo plantea Paniamor/IIJusticia/SCS, (2009) es necesario partir de la premisa de que si bien, existen una serie de condiciones en la web que potencian la manifestación de distintas expresiones de la violencia, el problema no radica en la herramienta propiamente, sino en el uso que las personas adultas y menores de edad hacen de ella. En tanto, como lo afirma ECPAT (2005) "el ciberespacio refleja las mismas polaridades de la conducta humana que se pueden ver en los espacios físicos, donde los niños y adolescentes son vulnerables al daño infligido por otros (pares y/o adultos)..."

Ello plantea por tanto, una legítima preocupación en relación al impacto que las TIC puedan acarrear a poblaciones particularmente vulnerables, así como de las acciones que desarrollen o no los actores sociales garantes de derechos de acuerdo a sus mandatos y obligaciones legales, en función de desarrollar mejores estrategias personales y colectivas de protección y autoprotección en la red.

En este sentido, el análisis de la vulneración de derechos de las personas menores de edad, mediada por las TIC, requiere un abordaje integral y contextualizado, que permita dibujar el entramado complejo de relaciones que exceden planteamientos de causa y efecto; y comprender la complejidad y multifactorialidad del problema, para proponer acciones concretas que fortalezcan en las personas menores de edad, aquellos conocimientos, actitudes y prácticas que permita el disfrute y aprovechamiento pleno de estos recursos, así como el ejercicio de una ciudadanía digital con capacidad de transformación social en este nuevo contexto social.

1. De la preocupación a la ocupación y a la articulación...

No basta entonces, con limitarse a la identificación del problema, hay que idear y llevar a la práctica estrategias innovadoras, pertinentes y efectivas para solucionarlo; vinculando en este proceso, a los actores sociales que en función del contexto, sus mandatos y capacidades de acción, se vean interpelados.

A la luz de esta premisa, surge en 2009 el proyecto *Derechos y Justicia en el Movimiento Social en Internet* (DJMSI), una iniciativa regional de investigación aplicada que desarrolló acciones especificas en doce países de América Latina; siendo formulado y ejecutado por el Instituto de Investigación para la Justicia (IIJusticia) con sede en Buenos Aires, Argentina, y financiado por la Agencia Canadiense de Cooperación (IICD/IDRC).

Por la naturaleza de los efectos e impactos que se propuso alcanzar, el proyecto fundó su método, en la integración crítica de conocimientos y regulaciones disponibles en los contextos sociales donde operó, así como en la construcción de consensos mediante la sensibilización de actores sociales con influencia en la generación de programas de políticas públicas (Terneus, 2009).

La iniciativa enfocó sus esfuerzos a explorar y desarrollar una base de conocimiento que, incluyera analíticamente, una sistematización de los riesgos y una síntesis actualizada de las soluciones ensayadas en relación con los derechos fundamentales en Internet, en especial la privacidad (entendida como paradigma), orientada a facilitar un debate informado sobre los riesgos generados por las TIC en poblaciones vulnerables (especialmente niños, adolescentes y jóvenes) y sus posibles correcciones, manteniendo siempre los logros de acceso a la información, libertad de expresión y transparencia del Estado y las instituciones.

Para cumplir con sus objetivos, el proyecto operó bajo una propuesta metodológica articulada por tres etapas secuenciales: (i) Investigación, (ii) Construcción de Consenso, e (iii) Incidencia Política, información y concientización de usuarios. Cada una de estas etapas, involucró la participación de un amplio conjunto de actores sociales, enfatizando la participación específica de cada uno, de acuerdo a los procesos y orientaciones individuales de la etapa particular.

Entre los involucrados en estas etapas, se citan investigadores y conocedores del tema, con una participación orientada hacia el planteamiento y la socialización de ideas y contenidos; ONG´s y otros grupos sociales, en función de generar discusión, reflexión y construcción de consensos; formuladores de políticas públicas; personas adolescentes y sus referentes adultos en el ámbito educativo, así como otros actores con condiciones y licencias jurídico-sociales para la toma de decisiones de Estado.

Fue en el marco de este proyecto que en 2009 se desarrolló una convocatoria abierta a investigadores de América Latina y el Caribe para proponer temas pertinentes al uso de la privacidad en Internet, siendo seleccionado el estudio Colombiano "Significados e implicaciones del protagonismo sexual de adolescentes de provincia en la Internet" desarrollado por Zareth Díaz y Raúl Rojas. El cual, dio cuenta de algunas de las características de las Instituciones Educativas Departamentales de Cundinamarca (IEDC) y de su cuerpo docente, frente a la formación de NNA para prevenir los riesgos en la internet, concluyendo principalmente que:

> – El sistema educativo no estaba preparado en cuanto a estrategias y conocimientos para asumir la tarea formativa que le compete en el uso seguro y responsable de las TIC.
>
> – No se percibía un interés por parte de las IEDC y sus profesores en aprender sobre estos riesgos, e incorporarlos como parte integral de la formación de NNA.
>
> – Se percibía en las IEDC que las situaciones de riesgo de sus estudiantes en Internet, eran ajenas al contexto educativo.
>
> – Los fenómenos de riesgo y vulneración de derechos presentados en las IEDC se trataban de manera correctiva, solucionando coyunturalmente la situación, especialmente con sanciones a quienes participaban (como victimas y/o victimarios) de estas acciones.
>
> – La sistematización de las acciones tendientes a la formación de NNA para el uso seguro y responsable de las TIC por parte de instituciones Educativas y profesores de provincia, era casi inexistente, con tendencia a la repetición de éxitos o fracasos, ya que no existían registros ni mucho menos las evaluaciones de ellas, por ende, sin posibilidad de estimar

cuáles aspectos reforzar y cuáles no, cómo actuar o no. En este sentido era común la improvisación para enfrentar estos fenómenos.

Estos hallazgos, planteaban –para el caso particular de Cundinamarca en Colombia, pero fácilmente extrapolable a toda región y más allá– una problemática, no totalmente reconocida como de urgente abordaje por parte la institucionalidad educativa responsable de propiciar medidas de protección, principalmente en aquellas poblaciones con mayores niveles de vulnerabilidad.

En este sentido, el Sistema de Educación Formal está llamado a asumir un rol protagónico como agente transformador y garante de derechos, mediante el desarrollo acciones estratégicas e innovadoras de información-formación que vinculen a la población menor de edad en el desarrollo y fortalecimiento de su propias estrategias de protección y autoprotección en este nuevo contexto.

Ante este panorama, el proyecto DJMSI asumió una actitud propositiva, dinamizando las condiciones necesarias para construir una alianza estratégica con la Secretaría de Educación del Departamento de Cundinamarca, con el objetivo de implementar una experiencia educativa concreta, diseñada para abordar esta situación, desde el rol que le corresponde a la Educación Formal, como formadora y garante de derechos.

Es así como el 8 de enero de 2010, mediante convenio firmado entre las partes, se oficializa el proyecto denominado "Protección de la privacidad y datos personales de los niños y adolescentes usuarios de la web", en el cual, la Secretaría de Educación se comprometía a brindar el apoyo logístico necesario para catalizar el desarrollo de la experiencia piloto en un conjunto instituciones de educación básica primaria, secundaria y media del sector oficial; que representaran riesgo por su cercanía a grandes ciudades capitales; que tuviesen influencia del turismo; del control de grupos al margen de la ley o con casos reportados de comportamientos no seguros en la red. Para ello el IIJusticia asumió el rol de gestor técnico-financiero de la iniciativa, que para sus efectos programáticos consistiría en una aplicación práctica de su etapa de Incidencia Política, información y concientización de usuarios.

En este sentido, el proyecto propuso como objetivo principal "Movilizar la participación protagónica de la Comunidad Educa-

tiva del Departamento de Cundinamarca en Colombia, así como de otros actores sociales del contexto nacional; en el desarrollo de acciones formativas y de incidencia, orientadas a la protección de la privacidad y los datos personales de las personas menores de edad en la web", valga acotar que esta iniciativa no contemplaba acciones directas en Bogotá.

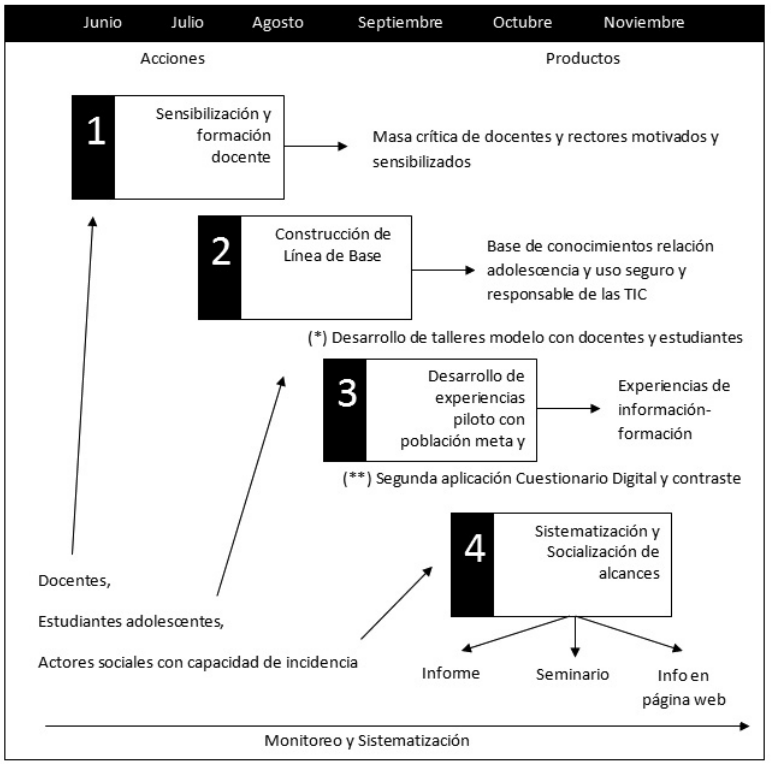
Para lograr este propósito, docentes y rectores capacitados en el tema, diseñarían e implementarían de manera autónoma una experiencia educativa piloto de sensibilización, dirigida a adolescentes activos en el sistema educativo formal. Llevada a cabo mediante acciones pertinentes, atractivas y movilizadoras, que fortalecieran en ellos y ellas, estrategias efectivas para la protección de su privacidad y datos personales en la web.

Este propósito significaba de entrada un reto en varias dimensiones, desde aquella relacionada con fortalecer en el equipo docente los enfoques adecuados para el abordaje del tema, hasta disipar temores adultos al no verse como referentes en esta temática, principalmente ocasionados por vacios de conocimiento y brecha digital generacional. Lo cual para el grupo docente, significaba una desventaja comparativa ante el mejor desempeño instrumental que en su mayoría referían las poblaciones adolescentes con las cuales iban a trabajar. Con estas aspiraciones y retos claros, dieron inicio las acciones concretas del proyecto.

2. Manos a la Obra...

Las acciones de campo fueron estructuradas en cuatro fases secuenciales, denominadas: sensibilización y formación docente; construcción de Línea de Base (LB); desarrollo de experiencias piloto con la población meta y el contraste de resultados; y finalmente, la sistematización y socialización de los alcances. Las actividades de cada una de estas fases se llevaron a cabo entre junio y noviembre del 2010, como se expone en la siguiente figura.

Figura 1. Fases del proyecto durante el segundo semestre (2010).



Cada fase propuesta, aportaría insumos para construir y fortalecer en las poblaciones meta, un conjunto de saberes acerca de la relación que establecen NNA con las TIC –principalmente la Internet– en términos de oportunidades y riesgos; roles de protección y autoprotección, factores y conductas protectoras y de riesgo; entre otras. Ello con la aspiración de incidir en enfoques, metodologías, conocimientos, actitudes y prácticas de los grupos sociales involucrados, específicamente en el área temática de interés.

Valga reconocer que el desarrollo de estas fases fue posible, gracias al compromiso y motivación del grupo de docentes y rectores que asumieron el reto de construir las condiciones locales necesarias para cumplir con los objetivos propuestos, participando desde sus comunidades como equipos de multiplicación y resonancia con gran suceso. Hagamos entonces, un recorrido por esta experiencia educativa.

La primera fase consistió en un encuentro de sensibilización y formación para docentes y rectores de 26 municipios periféricos del área de influencia del proyecto, realizado entre el 8 y el 10 de junio de 2010 en la localidad de Chinauta. Este espacio sirvió de marco, para construir una aproximación acompañada, propositiva y concreta al problema de la vulneración de la privacidad y la exposición de datos de personas menores de edad mediante las nuevas TIC, particularmente aquellas ligadas a la web 2.0.

Para lograrlo se brindaron los insumos necesarios para la reflexión personal y grupal en torno al reconocimiento de las oportunidades y desafíos que plantean las TIC, el rol de garantes de derechos que tienen aquellas personas que disfrutan de estos recursos, así como aspectos éticos y el abordaje del tema desde el enfoque de derechos, encontrando en los asistentes un deseo genuino de profundizar y aprender más sobre el tema, así como un compromiso expreso de asumir el reto que el proyecto ofrecía.

Durante el encuentro se diseñó de manera conjunta una estrategia global que serviría de orientación docente para el desarrollo de las experiencias educativas piloto en los colegios participantes, principalmente diseñada para responder a dos interrogantes: ¿cómo plantear acciones con la población adolescente en este tema?, pero además desde ¿dónde hacerlo en términos ontológicos?

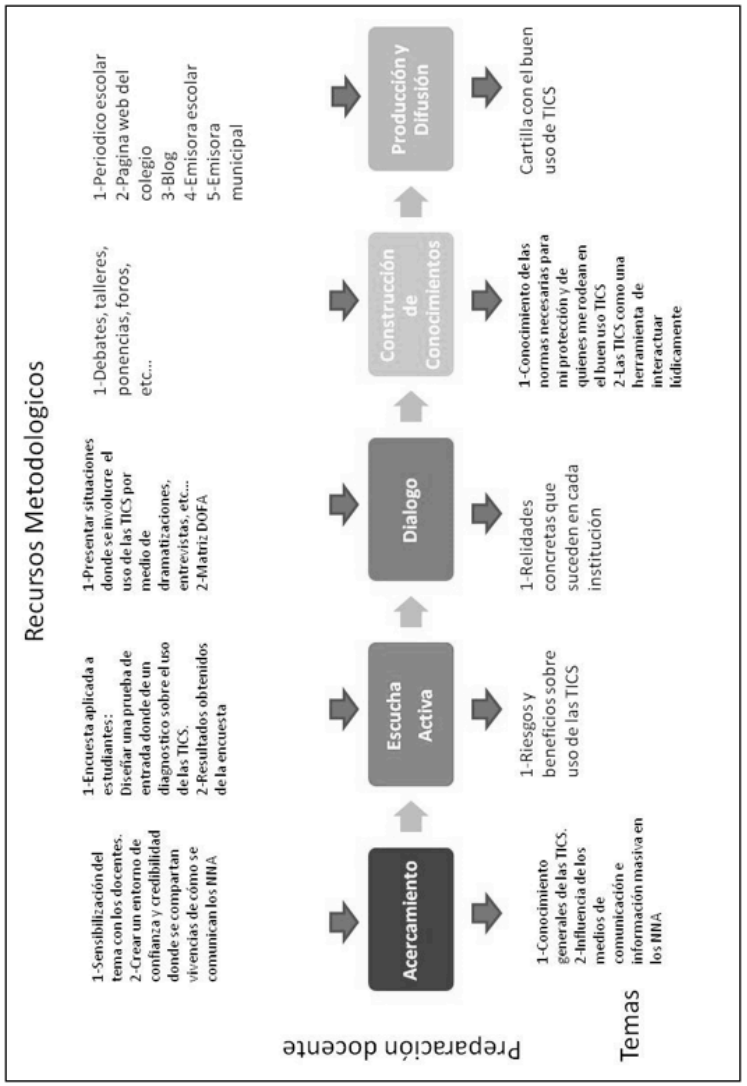
Para lograrlo, se construyó como primer producto, un decálogo de consideraciones docentes para diseñar e implementar experiencias educativas que fortalecieran en NNA estrategias personales de protección y autoprotección en la web, como recurso que sustentaría el enfoque docente para el abordaje del tema. Este conjunto de consideraciones se presentan en la siguiente figura.

Figura 2. Decálogo de Consideraciones Docentes.

1	Reconocer el contexto sociocultural de la comunidad en función del uso social de las TIC
2	El ciberespacio es un Espacio Público, con potencial para acceder a nue vas oportunidades y riesgos
3	Los actores sociales son garantes de derechos en cuanto al uso Seguro y Responsable de las TIC
4	Educar y fortalecer en *competencias ciudadanas*
5	La ética pilar fundamental
6	Debe fortalecer siempre la dignidad humana
7	Todas las acciones en el mundo digital tienen impacto en las dimensio nes de lo físico y emocional
8	Reconocer y validar los intereses de los actores
9	Evidenciar los procesos y resultados
10	Compromiso interinstitucional dentro de un marco legal adecuado

Como segundo producto, fue estructurada una estrategia de intervención conformada por un proceso secuencial articulado por cinco momentos metodológicos, el cual partía de un primer acercamiento horizontal al grupo meta; seguido por fortalecer la escucha activa por parte de los docentes; la construcción de un proceso de dialogo intergeneracional entre estudiantes, sus pares y profesores; el fortalecimiento colectivo de estrategias de protección y autoprotección en la web; y la socialización creativa a terceros de los resultados de estos procesos. En la siguiente figura se presenta a manera de ejemplo, una de las propuestas desarrolladas por las y los docentes participantes en el encuentro.

Figura 3. Propuesta de la Zona del Gualivá "El Uso Adecuado de Las Tics en NNA". Integrantes: Utica-Estela Cáceres –Rectora, Nelly Bohorquez-Docente Quebradanegra-Arnulfo Vargas-Rector, Estela Florian-Coordinadora, Villeta-Rosa Castro-Rectora; Adriana Marroquín-Docente, La Vega-José Aimer Ospina-Rector, Edgar Salamanca-Docente.



Procurando en todo el proceso, mejores conocimientos, actitudes y prácticas de protección en la web en las y los adolescentes vinculados a las acciones formativas; así como, docentes informados y con mejores capacidades de respuesta y acompañamiento a estas poblaciones en el marco de las oportunidades y desafíos que plantea la sociedad actual.

En este sentido, el encuentro procuró además, la formulación de las acciones concretas a implementar en cada uno de los centros educativos por parte de los docentes y rectores, para lo cual se generaron sesiones acompañadas de planificación. Valga reconocer que no todas las acciones propuestas, se centraron a trabajar con adolescentes, algunas de las acciones reconocían como pertinente y necesario, el trabajo directo con otros actores locales, como aquellos con poder para la toma de decisiones e incidencia política, tales como padres y madres de familia, el cuerpo docente, autoridades municipales y otros grupos de personas adolescentes.

Como estrategia exitosa de la gestión del encuentro, se tiene la participación articulada de al menos un docente y el rector o rectora por cada institución educativa involucrada, lo que fue decisivo en términos de la sostenibilidad de los procesos durante los seis meses siguientes. Lo cual, se debió directamente a la intermediación de la Secretaría de Educación que dio el aval institucional para congregar a esta población durante tres días laborales completos.

Posterior al encuentro, y como estrategia para generar un proceso continuo, articulado, colaborativo y público para la reflexión e información sobre el tema de fondo, se conformó un grupo virtual que funcionó como canal de comunicación durante toda la experiencia educativa. Mediante este canal se generó la mayor parte del acompañamiento técnico. Así mismo, fue un medio que aportó a la movilización y el mantenimiento de la motivación y para la reafirmación del compromiso asumido por el cuerpo docente, complementaria a las acciones de la Secretaría de Educación con este mismo objetivo. Este recurso virtual facilitó el intercambio de experiencias y materiales, la validación de instrumentos, el seguimiento de las acciones y la reflexión de manera asincrónica con y entre las y los docentes y rectores involucrados.

La segunda fase, planteaba conocer ¿cuál era la realidad de las y los estudiantes adolescentes de secundaria de los municipios

participantes, en términos de su relacionamiento con las tecnologías digitales, particularmente en lo que a conocimientos, actitudes y prácticas para el uso seguro y responsable de las TIC se refería?, por cuanto, sí el proyecto proponía una iniciativa que buscaba mejorar estas capacidades, el proyecto tendría entonces, que diseñar un mecanismo para medirlo.

Así, conocer cuál era la Línea de Base (LB) de la población adolescente en este particular, pero además mediante qué estrategia conseguirlo, devino en un conjunto de tareas que contaron con el aporte significativo vía virtual de las y los docentes involucrados, principalmente en términos de su validación y aplicación. Esta información por levantar, además de servir como punto de partida para conocer la realidad mencionada, serviría luego como base de contraste para la valoración de resultados y avances del proyecto en términos del cumplimiento de su propósito.

Valga mencionar que desde el principio fue evidente que la pluralidad de características de la población meta y el amplio contexto geográfico del proyecto, serían un elemento a tomar en cuenta para el levantamiento de la LB, por lo que era necesario definir una estrategia costo eficiente, científicamente sustentada y de *"fácil"* aplicación que aportara información relevante. Para cumplir con esta tarea se acordó emplear como técnica un cuestionario en línea, detonándose entonces, dos procesos paralelos: la construcción y validación del instrumento y el diseño y conformación del marco muestral.

El instrumento denominado *Hablemos de Internet*, consistía en un cuestionario auto administrado de aplicación virtual bajo la modalidad de muestra controlada, creado como herramienta científica para valorar diferentes grados de conocimientos, actitudes y prácticas relacionadas con conductas de riesgo y protección en la web de personas adolescentes.

El cuestionario tenía cinco secciones con preguntas de opción múltiple, escalas de *Likert*, escalas de frecuencia y preguntas para la caracterización de la población. Este cuestionario fue revisado y validado tanto por personas adolescentes como por personal docente, con el fin de depurar aspectos como comprensión del lenguaje, extensión y duración de aplicación, intencionalidad de los *items*, etc.

En cuanto al diseño muestral, este fue delimitado principalmente por tres criterios: grado de conectividad (Conexiones de banda ancha y angosta reportadas por municipio en 2009);[1] sexo y edad (distribución de población por municipios según censo 2005 y proyecciones al 2010);[2] así como por región (proyección de población urbana y rural al 2007).

La muestra fue construida y segmentada según la composición porcentual de los criterios mencionados, según municipio. Procurando obtener una muestra representativa de personas adolescentes con las características de la población. Para lo cual se propuso contar con una muestra superior a las 400 personas, que en términos estadísticos representaría un 5% de error de muestreo.

De seguido vino la aplicación virtual del instrumento, el cual fue respondido por 439 adolescentes. Para lograr este resultado, cada centro educativo generó las condiciones para seleccionar la muestra según la cantidad y características que le correspondía según el diseño; así mismo gestionó las condiciones y los espacios de conectividad dentro del ámbito escolar o en el contexto comunitario. A manera de anécdota que refleja el compromiso asumido por el cuerpo docente, se tiene el caso de un centro educativo que al tener serios problemas de conectividad en su institución, prefirió, antes de retirarse del proceso, salir con las y los adolescentes y un grupo de docentes acompañantes a tres diferentes café internet de la comunidad cercana al colegio, para cumplir con el compromiso y el calendario propuesto, un ejemplo sin lugar a dudas, como estas hay otras anécdotas que reafirman el nivel del compromiso asumido por el cuerpo docente.

La información de la línea de base, el decálogo propuesto, la estrategia global y las propuestas de acción esbozadas en el encuentro de sensibilización y formación docente sirvieron como insumos para el desarrollo de la siguiente fase, que consistió en la implementaron de las experiencias piloto en cada uno de los centros educativos involucrados.

[1] *Sistema de Información Unificado del Sector Telecomunicaciones* – SIUST de Colombia. Dicha información puede consultarse en la dirección www.siust.gov.co, a través del enlace denominado Cifras del Sector.

[2] Gobernación de Cundinamarca, *Secretaría de Planificación Población rural y urbana*. Cifras proyectadas por municipio, 2007.

Para esta fase cada nodo de gestión educativa[3] hizo valer su compromiso de proponer, construir y aplicar diversas estrategias de información acción; en principio para un grupo piloto de de entre 20 y 40 adolescentes. No obstante, como fue comentado de previo, el efecto de *bola de nieve* impulsado por el proyecto, provocó que durante el desarrollo de las acciones se llegase a vincular a muchas más personas adolescentes y otros docentes del entorno educativo, así como padres y madres de familia, y líderes locales, lo cual amplió significativamente el rango de cobertura esperado.

Cada una de las estrategias implementadas en lo local, respondió a una lectura de viabilidad y pertinencia asumida enteramente por los nodos de gestión, en función de lo que fue considerado por ellos con de mayor potencial de éxito para sus contextos, su capacidad de movilización de recursos, pero sobre todo su inventiva y creatividad.

Un elemento fundamental que no debe perderse de vista, en cuanto a la intencionalidad del proyecto, es el énfasis en concientizar y movilizar actores sociales, desde el reconocimiento de sus propias capacidades como garantes de derechos de NNA frente a sus interacciones con las TIC. Lo cual, en el caso de los actores educativos, se lleva a la práctica mediante la implementación de procesos y acciones formativas que, además de llevarles a descubrir sus propias estrategias de actualización y aprendizaje continuo sobre el particular, les lleve a diseñar junto con la población estudiantil acciones pertinentes, vinculantes y atractivas, que generen los efectos de protección y autoprotección ya mencionados.

Como se verá en el apartado de resultados, la gama de experiencias educativas desarrolladas fue bastante amplia, lo que le dio al proyecto un matiz especial entre lo experimental y lo creativo, entre lo formativo y lo informativo y entre lo personal y lo colectivo, que lo vuelven muy particular, lo que sin duda alguna despertará nuevas reflexiones e interrogantes para desarrollar y responder.

Para cerrar la fase de implementación de experiencias, se quiso conocer -en los mismos términos de la LB- el perfil de salida de las personas adolescentes que participaron en el proceso previo completo (LB y experiencias educativa piloto), con el fin de valorar

[3] Concepto con el que se nombraron los equipos de trabajo en cada centro educativo, conformados por al menos un rector(a) y un docente responsable.

el mejoramiento o no de sus conocimientos, actitudes y prácticas de protección en el ciberespacio por intermediación de las acciones vinculadas al proyecto.

Para lograr este comparativo, se desarrolló una nueva aplicación del cuestionario virtual, de manera que la valoración de éxito se fundamentó en la aplicación de una técnica de contraste *exante-expost,* que dio pie de manera científica a reconocer con un 95% de confiabilidad, el nivel de mejora o no en dichas dimensiones de análisis.

Finalmente, la cuarta fase del proyecto contempló la sistematización y socialización de la información y resultados obtenidos durante las fases anteriores, para lo cual, se construyó un documento de registro y valoración global de resultados, avances y lecciones aprendidas denominado Informe de Resultados, presentado y entregado oficialmente a la Secretaría de Educación de Cundinamarca en noviembre del 2010.

3. Un vistazo a los resultados...

Más allá de los resultados en el ámbito de la gestión o del desarrollo metodológico emanados de la experiencia de capacitación y formación inicial, se tiene como elemento fundamental, la sensibilización de 50 rectores y docentes en términos del reconocimiento de su capacidad para asumir papeles activos y protagónicos en la construcción de procesos de información-formación –en este particular tema– desde el contexto educativo formal, diseñados para que las y los adolescentes construyan sus propias estrategias para el aprovechamiento, protección y autoprotección en sus interacciones sociales en Internet.

Así mismo, también cuenta como resultado, el reconocimiento por parte de este grupo de un conjunto de enfoques que perfilan el abordaje de este tema desde lo educativo y no desde lo prohibitivo; desde lo cultural y no únicamente desde lo tecnológico; desde su potencial y no sólo desde sus carencias; así como desde el reconocimiento de las nuevas tecnologías como nuevos contextos de socialización y construcción de identidad, importantes para las personas menores de edad, útiles para la construcción de ciudadanía

activa y para la reivindicación de derechos, pero igualmente validas para el ocio y el entretenimiento. En resumen, una realidad que debe ser acompañada, en función del desarrollo de las mejores capacidades para el disfrute pleno de las oportunidades que ofrecen y la prevención del riesgo, una responsabilidad que sin duda toca también al Sistema Educativo Formal.

Por otro lado, como resultado principal de la LB se tiene, una plataforma de conocimiento generada en agosto 2010, sobre la realidad de adolescentes estudiantes de secundaria, habitantes en municipios periféricos del departamento de Cundinamarca en Colombia, sobre su relación con la Internet, principalmente en términos de sus conocimientos, actitudes y prácticas de protección y seguridad en sus interacciones virtuales. Información con el potencial de nutrir acciones nuevas y más focalizadas sobre el tema.

La línea de base estuvo conformada por la participación de 439 adolescentes: 118 hombres y 121 mujeres con edades entre 12 y 15 años, y 98 hombres y 102 mujeres con edades entre 16 y 18 años, en su mayoría (67%) con características urbanas. Una lectura breve de la información obtenida permite observar:

3.1 Valoración a partir de información general

– El 60% de la población consume Internet entre 5 y más de 20 horas a la semana.

– En casi todas las agrupaciones de tiempo de consumo, sobresalen los porcentajes asociados a las mujeres adolescentes en comparación con sus pares valores, no obstante tales diferencias, se van acortando, conforme aumenta el tiempo de exposición.

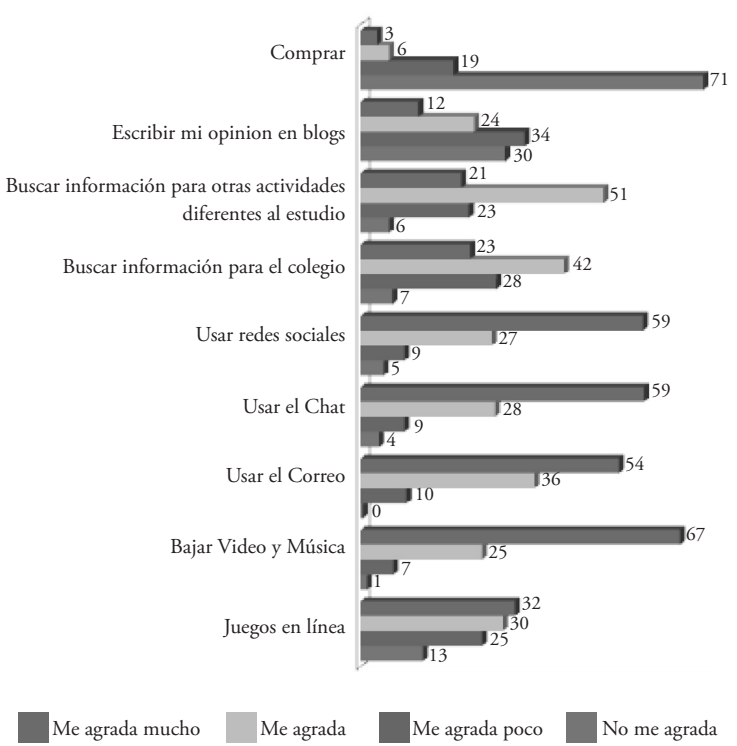
– Un 48% de los participantes posee conexión en el hogar, el resto lo hace en espacios públicos o familiares, siendo el colegio el espacio en el que menos acceden a este recurso.

– Un 51% asevera utilizar la internet cada vez que lo desea, el resto presenta algún grado de condicionamiento respecto a su uso, principalmente asociados a la autorización adulta o a la capacidad de pago en café internet.

– Los usos de internet que poseen las valoraciones de agrado

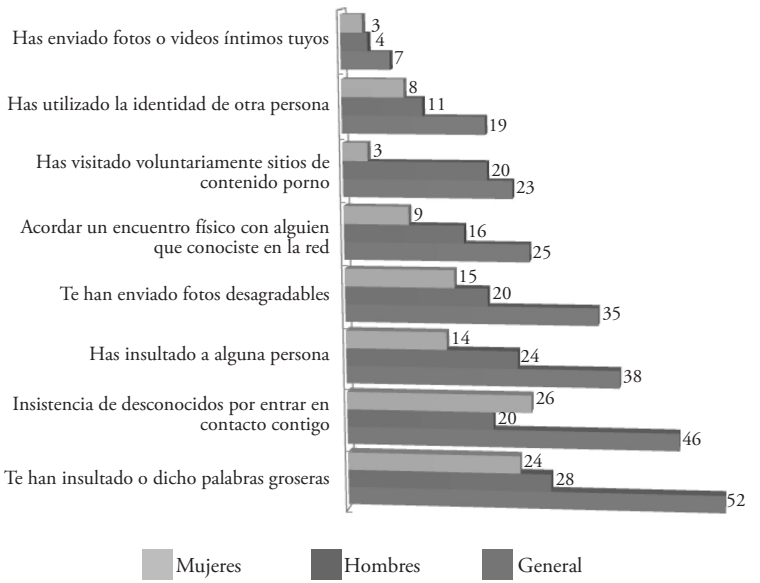
más altas son aquellas asociadas con la socialización, comunicación y entretenimiento, en contraposición con aquellas relacionadas con educación, expresión y socialización de sus ideas, que presentan las valoraciones de menor agrado, lo cual se puede apreciar con mayor detalle en el siguiente gráfico.

Gráfico 1. Porcentaje de personas adolescentes participantes en la línea de base según preferencia por servicios web. Proyecto Protección a la Privacidad y Datos Personales de NNA, Cundinamarca, Colombia, septiembre 2010.



El gráfico siguiente refleja situaciones de vulnerabilización y riesgo en las personas adolescentes participantes en el estudio en el lapso de los 30 días previos a la aplicación del cuestionario.

Gráfico 2. Porcentaje de personas adolescentes participantes en la línea de base según situaciones de victimización en Internet en el mes previo a la aplicación del cuestionario. Proyecto Protección a la Privacidad y Datos Personales de NNA, Cundinamarca, Colombia, septiembre 2010.



– A partir del cual se observa que el mayor porcentaje (52%) está relacionado con la recepción de insultos y palabras groseras en las interacciones virtuales (*Flamming*).

– El 46% de los encuestados han recibido la insistencia de desconocidos por entrar en contacto con ellos y ellas en la red, lo cual es más intenso en el caso de las mujeres.

– Un 35% de las y los jóvenes reporta haber recibido fotografías con contenido desagradable, lo que es mayor el caso de los varones adolescentes.

– El 25% reconoce haber acordado de encuentros físicos con personas que conocieron en la red, lo que se da con mayor fuerza en el caso de los varones adolescentes.

– Otras formas de riesgo, de menor incidencia en esta población pero de no menor ocupación, lo conforman la visita a sitios de contenido pornográfico, uso de la identidad de otra persona y la publicación de videos íntimos personales.

3.2 Valoración a partir de los índices

Para agrupar la información, se construyeron índices para cada una de las dimensiones de análisis (conocimientos, actitudes y prácticas), los cuales fueron desagregados en subescalas a partir de la información aportada según diferentes agrupaciones de preguntas en el cuestionario. La tabla 1 muestra los indicadores que operacionalizan cada una de las subescalas, que a su vez representan preguntas o combinaciones de ellas en el cuestionario empleado.

Tabla 1. Escalas de evaluación según indicadores.

Escala	Subescala	Indicadores
Conocimientos		- Grado de conocimiento que los adolescentes refieren sobre Internet como sitio abierto de interacción social con potencialidades y riesgos - Grado de conocimiento que internet es una herramienta que permite el acceso abierto a la información e interacción sin limitaciones geográficas o de grupo
	Ciberespacio	- Grado de reconocimiento del anonimato y la fabricación de identidades como una de las características de la red - Grado de conocimiento de la existencia de legislación vigente en Colombia sobre el tema de protección de derechos y TIC - Grado de conocimiento de los mecanismos y los espacios de denuncia en caso de una afectación personal o de su grupo de pares mediada por internet
Actitudes	Expresiones de Violencia	- Grado de reconocimiento el concepto de acoso en línea en su contexto personal y social - % de adolescentes que reconocen la existencia de casos de acoso en línea en su contexto personal y social
		- % de adolescentes que reconoce la existencia de casos de sextina en su contexto personal y social - Grado de reconocimiento del riesgo asociado a prácticas de preparación en línea - Grado de exposición a contenido no deseado como un riesgo durante sus interacciones virtuales - Grado de reconocimiento de prácticas que comprometan la seguridad de sus datos personales y su privacidad en internet - Grado de reconocimiento de conductas personales de protección frente a situaciones de *Flamming* - Grado de reconocimiento de situaciones de riesgo frente a situaciones de solicitación sexual
	Uso significativo	- Grado de predisposición a actuar de forma segura en sus interacciones virtuales - % de adolescentes que reconocen la red como medio de superación y de expresión individual
	Autoprotección	- Grado de predisposición para contar con referentes adultos de confianza como apoyo para fortalecer acciones de autoprotección - Grado de reconocimiento de la existencia de expresiones de violencia en la web
	Autorregulación	- Grado de predisposición a controlar el tipo de interacción y de contenidos a los que tienen acceso durante sus interacciones virtuales
	Protección del grupo de pares	- Grado de predisposición para asumir el rol de garante de derechos del grupo de pares
Prácticas	Control del Riesgo	- % de adolescentes que incurren en prácticas de riesgo durante sus interacciones virtuales
	Autocuidado	- % de adolescentes que implementan practicas de protección durante sus interacciones virtuales

La información obtenida de las respuestas de la LB, fue procesada estadísticamente[4] con el fin de obtener análisis de frecuencias y tablas de contingencias según características socio -demográficas de las y los adolescentes, así como por variables relacionadas al constructo de uso seguro y responsable de internet. Algunas de las valoraciones obtenidas son las siguientes:

– *En términos de conocimientos*: las ponderaciones evidencian un nivel relativamente bajo para esta escala, con una valoración que apenas llegó al 50,96% en una escala de uno a cien. Desagregando este indicador, se reconoce que la población encuestada reportaba mejores conocimientos sobre el ciberespacio, que aquellos relacionados con la identificación de expresiones de violencia en este contexto.

Esto puede deberse a que las y los adolescentes como usuarios intensivos de las TIC, están en mayor medida familiarizados con aspectos técnicos y con las características del contexto virtual, que con aquellos conocimientos que les permita la identificación de expresiones de violencia en sus interacciones en la red. Esto deviene en un factor de vulnerabilidad que requiere ser atendido desde las instancias y mediante los procesos que enmarcan la protección de las personas menores de edad desde un enfoque de derechos. En términos generales se pudo afirmar además, que las mujeres adolescentes tenían mejores niveles de conocimientos que sus pares varones. Las otras variables no mostraron diferencias significativas.

– *En términos de actitudes*: las actitudes reflejaron el valor más bajo de las tres escalas del estudio con un 49,50%, su desagregación en subescalas mostró que la población adolescente encuestada presentaba mejores niveles de actitudes personales hacia el uso significativo de las TIC; que aquellas, hacia la autoprotección en la web, la protección de pares y mucho mayores que aquellas relacionadas con su auto regulación en este contexto.

[4]Para comparar los promedios de sexo y grupo etario, por tratarse de una variable continua en dos categorías se utilizó el procedimiento basado en la distribución 't' de *Student*, para el caso de la procedencia geográfica, se empleo el análisis de varianza ANOVA basado en un factor.

En este sentido, las mujeres reflejaron los mejores niveles en todas las subescalas de actitudes en comparación con los hombres, sobresaliendo en lo particular en la subescala de protección hacia el grupo de pares. Las y los adolescentes con edades entre 16 y 18 años mostraron mejores niveles en cuanto a las actitudes hacia el uso significativo, la autorregulación en el ciberespacio y el seguro y responsable de las TIC; que aquellos adolescentes con edades entre 12 y 15 años.

Finalmente en cuanto a la zona geográfica, si se reconocieron diferencias significativas entre los adolescentes de comunidades urbanas, quienes reflejaron mejores actitudes para la autorregulación, que aquellos, de comunidades rurales y de comunidades semiurbanas, estos últimos obteniendo la menor ponderación.

– *En términos de prácticas*: este índice reflejó el valor más alto de todas las escalas con un 52.14%. En cuanto a los valores de los índices de las dos subescalas que conforman este indicador: prácticas de control de riesgo y prácticas relacionadas con autocuidado estos presentaron la más alta y la más baja ponderación del estudio.

En términos de género las mujeres adolescentes reflejaron las mejores prácticas de control de riesgo y autocuidado que sus pares varones. Así mismo, dentro del grupo de las mujeres, ellas muestran diferencias muy significativas a favor de las prácticas de control del riesgo, en contraste con sus propias practicas de autocuidado. Las otras variables no muestran diferencias significativas.

Una vez levantada la LB, iniciaron las acciones en los centros educativos de los municipios participantes, las cuales fueron catalogadas en tres categorías principales, aquellas diseñadas para la información, para la formación y para la movilización de actores sociales clave. No obstante, en pocos de los casos se desarrolló una única de estas posibles orientaciones, por el contrario, la media de los centros educativos implementaron combinaciones de ellas.

En este sentido, la gama de iniciativas reportadas fue bastante amplia, incluyendo acciones como: concursos de vídeo en línea, talleres y charlas para la información y sensibilización, diseño y publicación de carteleras educativas, producción y distribución de material impreso y digital, creación de manuales para la seguri-

dad en línea, creación y mantenimiento de grupos y perfiles en redes sociales, desarrollo de *blogs*, materiales audiovisuales, reuniones con líderes locales, acciones de incidencia en cafés internet, diseño de aplicaciones para la promoción del uso seguro y responsable en Scratch, entre otras.

Valga mencionar que estas acciones involucraron la participación adolescente en todo momento, desde un planteamiento de co-gestión del proceso, lo que aportó no sólo a su sensibilización sobre el tema, sino al fortalecimiento de competencias y liderazgos, en el marco de la mediación y el acompañamiento generado por el equipo docente.

Asimismo, varias acciones con amplia cobertura fueron desarrolladas de manera paralela a la experiencia piloto, involucrando en algunos casos, la totalidad de las personas de la comunidad educativa de referencia, en otras palabras algunos equipos asumieron el reto de ampliar los procesos de información a toda su institución o instituciones vinculadas, así como a otros grupos sociales de su contexto municipal de referencia.

Por la lógica de acción asumida por el proyecto, no se plantearon instrumentos de seguimiento cuantitativo, no obstante cálculos informales (fácilmente certificables) dan cuenta de no menos de 5000 personas involucradas, entre las que se citan personas adolescentes, docentes, personal administrativo, padres y madres de familia, lideres municipales, propietarios de café internet, entre otras personas alcanzadas por las estrategias del proyecto y aquellas paralelas pero con importante valor agregado. En este sentido, si se retoman las comunicaciones y conversaciones informales con los nodos de gestión educativa, esta cifra bien podría resultar bastante conservadora.

No obstante, en apego estricto a los datos consignados de manera formal, se reportan al menos 332 adolescentes participantes en todas las fases del proyecto, así como un mínimo de 50 profesionales en educación entre docentes y rectores, aunque como ya fue mencionado es posible afirmar que estos datos son mucho menores a la cobertura real alcanzada.

En el mes de octubre 2010, posterior al desarrollo de las experiencias piloto, toco el turno de realizar una nueva valoración de la población adolescente en términos de identificar posibles cam-

bios en cuanto a conocimientos, actitudes y prácticas.

La valoración se realizó bajo las la misma estructura que la línea de base, para ello se tomaron en cuenta únicamente personas adolescentes que hubiesen participado en las dos fases previas, de manera que la identificación de tales cambios –de percibirse- pudiesen ligarse a los procesos de información-acción desarrollados.

En este sentido, como fue indicado anteriormente, el objetivo de esa segunda aplicación del cuestionario, era contrastar las valoraciones obtenidas por la muestra en términos de los índices de conocimientos, actitudes y prácticas, una vez desarrolladas las acciones concretas en cada municipio. Lo cual, aportaría un respaldo científico-estadístico respecto del logro del objetivo perseguido.

Valga mencionar que en la segunda aplicación del cuestionario contó con la participación de 332 adolescentes de 14 de los 19 municipios que originalmente aportaron datos a la línea de base, ya que causas externas al proyecto imposibilitaron la participación de la muestra inicial. Por lo cual este grupo es considerado como la población final del estudio.

Algunas de las valoraciones emanadas de la segunda aplicación y su contraste con la línea de base son las siguientes:

– Se aprecia una diferencia positiva (crecimiento) en todas las escalas de valoración general, lo que permite aseverar que en cuanto a conocimientos, actitudes y prácticas relacionadas con el uso seguro y responsable, el grupo adolescente evidencia un avance o mejora.

– En el caso de las sub escalas, todas excepto una, presenta el mismo comportamiento de crecimiento. La que no muestra un comportamiento creciente es aquella relacionada con las prácticas de autocuidado, que podría sugerir que la población adolescente reconoce como suficientemente seguras sus prácticas, no obstante desde el sustento teórico parecieran no ser suficientes.

– En promedio, el crecimiento en las escalas entre la primera y segunda valoración, ronda un intervalo entre el 1% y 5%, lo que podría considerarse un crecimiento poco significativo, no obstante hay que recordar que el tiempo de ejecución de los procesos no supero los dos meses.

– La muestra en términos de la variabilidad de las respuestas, refleja un comportamiento bastante similar en ambos momentos de aplicación.

– El caso de la subescala de actitudes hacia la autorregulación, es un caso particular importante de resaltar, ya que en la primera valoración reflejó la segunda menor valoración de todas las demás, con un valor de 40.99%. En la segunda aplicación, su valor llego a crecer hasta un 46.14% representando un incremento del 13% respecto del valor inicial, este incremento es el más significativo en comparación con los demás, lo que sustenta reconocerla como la dimensión de mayor crecimiento en todo el proceso.

– Lo anterior sugiere pensar que el proceso de reflexión desarrollado desde cualquiera de las estrategias implementadas, pudo haber calado con mayor profundidad en la reflexión individual de las personas adolescentes, acerca de la importancia de valorar su propio desempeño en la regulación de conductas y prácticas de riesgo en sus interacciones virtuales

– Otra subescala de crecimiento importante, es aquella relacionada con las actitudes de protección de grupo de pares, la cual aunque no en una dimensión tan amplia como la anterior, sí merece reconocimiento de avance, principalmente, en cuanto a lo que ello significa en términos del mejoramiento de las condiciones de seguridad de sus pares.

– Con la información recolectada, es posible desarrollar un estudio comparativo de mayor calado.

La figura siguiente resume los resultados de la primera y segunda aplicación del instrumento de medición de resultados, así como el incremento o no entre mediciones en términos porcentuales.

Figura 4. Resultados en términos de las valoraciones porcentuales de las escalas y subescalas de Conocimientos, Actitudes y Prácticas. Cundinamarca Colombia. Proyecto Protección a la Privacidad y Daros Personales de NNA, Cundinamarca, Colombia, noviembre 2010.

En el marco de la última fase del proyecto, fue organizado en noviembre de 2010 en Bogotá un seminario- taller para la presentación de resultados, el cual contó con la participación de varias delegaciones de estudiantes, docentes y rectores de los municipios involucrados, invitados especiales de centros educativos de Bogotá, especialistas en el tema de ciberseguridad de empresas privadas e instituciones públicas, autoridades de la Secretaría de Educación, entre otros. Este seminario sirvió de acción aglutinadora para entregar de manera oficial a la Secretaría de Educación de Cundinamarca el informe de resultados del proyecto desarrollado, esto con fines de incidencia en la consecución de nuevas acciones concretas en este tema, impulsadas desde este ente rector.

El informe final de resultados, artículos como éste y otras iniciativas de corte digital, son parte de los productos de esta última fase, diseñados con la intención de difundir la experiencia entre otros actores estratégicos de sectores de la educación, justicia, telecomunicaciones, empresa privada, entre otros, con fines de movilización e incidencia. Ello con el fin de motivar nuevas experiencias en este tema particular en el ámbito nacional colombiano, como en aquellos otros contextos internacionales interesados y con capacidad de réplica en el corto o mediano plazo.

A manera de cierre...

La experiencia educativa desarrollada cuenta con un registro bastante nutrido en términos de resultados cualitativos y cuantitativos alcanzados. Lo cual, permite catalogarla como exitosa en términos del cumplimiento de sus objetivos más estratégicos: Incidencia política, información y concientización de usuarios.

Además, valga indicar que a partir de la experiencia global se esgrimen un conjunto de recomendaciones para la Secretaría de Educación de Cundinamarca en procura de capitalizar el camino avanzado en materia de sensibilización. Algunas de estas sugerencias son:

– Dar seguimiento a los procesos de formación y actualización docente sobre el tema, así como a aquellos desarrollados desde las instituciones educativas de manera que, metodológicamente, se ensayen acciones concretas con los mismos estándares de acción, sin que ello represente forzar a la comunidad educativa a renunciar a su capacidad creativa

– Mapear en el entorno colombiano aquellos actores sociales y empresariales con capacidad e interés de construir alianzas estratégicas para llevar a escala la propuesta, o desarrollar nuevas acciones igualmente relevantes y pertinentes.

– Implementar procesos formativos para docentes y rectores en este tema, o vincularles con opciones de formación desarrolladas por terceros, ya sea de manera presencial o virtual, mejorando para ello, las condiciones de acceso y conectividad en los centros educativos participantes.

– Socializar las estrategias desarrolladas, mediante el uso de los medios tradicionales y virtuales de comunicación con que se disponga, reconociendo la acción protagónica de docentes y rectores, en la mejora de conocimientos, actitudes y prácticas de protección en la web por parte de NNA.

– Socializar los resultados del proceso y abrir nuevos canales de comunicación virtual con los docentes, como acción catalizadora para el desarrollo de nuevos procesos y la vinculación de nuevos multiplicadores.

– Capitalizar el trabajo intenso de la personas menores de edad en el desarrollo de las acciones de información y formación, y reconocerles como aliados estratégicos con capacidad de diseñar e implementar nuevos procesos de multiplicación entre sus pares.

– Se sugiere la formulación e implementación de un plan educativo oficial dirigido a las y los profesores de las Instituciones Educativas Departamentales de Cundinamarca, que sirva de sustento para el desarrollo de nuevas acciones de formación para NNA en el uso seguro y responsable de Internet.

Asimismo, desde un enfoque crítico, al ser ésta la primera experiencia de movilización social desde el ámbito educativo, impulsada por el proyecto *Derechos y Justicia en el Movimiento Social en Internet*, es evidente -como en toda experiencia piloto- la existencia de un conjunto de aprendizajes y de áreas de mejora, que permitan en una eventual replica desarrollar experiencias más robustas. Algu-

nas de estas consideraciones son:

– Hacer una revisión objetiva del modelo de acompañamiento técnico, para contextualizarlo y fortalecerlo desde lo local, pero no en detrimento del apoyo externo.

– Considerar la agenda del año lectivo y las coyunturas administrativas del sector educativo formal existentes o con potencial de existir, para reconocer los mejores periodos para la ejecución de las actividades de este tipo.

– Contar con un diagnostico de partida -no excluyente- de los conocimientos, actitudes y prácticas del cuerpo docente frente al uso seguro y responsable en la Internet, así como su incorporación o no en procesos formativos y experiencias previas sobre el tema.

– Contar con una lectura actualizada de las características propias de los contextos educativos, sociales y políticos de trabajo, en relación a la utilización de Internet y la influencia que reciben del comercio, el turismo o la economía.

– Analizar con mayor fuerza las estrategias educativas que se han desplegado en contextos similares y estudiar cuáles han sido sus resultados en la formación del conocimiento, prácticas y actitudes de NNA en el uso seguro y responsable en Internet.

– Hacer una valoración de la pertinencia y la efectividad de la propuesta metodológica con que operó el proyecto, frente a otros modelos.

Finalmente, lo conseguido por el proyecto en términos de resultados concretos, es producto de la articulación significativa de un conjunto de actores sociales que se vieron reflejados en todos los momentos de propuesta, y que desde lo institucional y lo local contribuyeron al logro de los mismos.

Estas fuerzas sociales estuvieron representadas en el plano nacional, por la Secretaría de Educación, las instituciones educativas, los docentes, rectores y estudiantes adolescentes, así como por todas aquellas personas alcanzadas en Cundinamarca; y representadas en lo internacional, por el apoyo financiero del Centro Internacional de Investigaciones para el Desarrollo (CIDA) y la Agencia Cana-

diense de Desarrollo Internacional (IDRC), así como por el apoyo técnico del Instituto de Investigación para la Justicia.

Cada uno de estos actores jugó un papel fundamental en la consecución de los resultados, comprobado que esta experiencia educativa particular, es un claro ejemplo de que la protección de la privacidad y datos personales de NNA en la web, es posible, pero es sin lugar a dudas, una responsabilidad compartida...

...en la cual como formadores tenemos un rol fundamental que asumir...

Bibliografía consultada

DIAZ, Z. y ROJAS, R. (2008), *Significados e Implicaciones del Protagonismo Sexual de los Adolescentes de Provincia en Internet*, Colombia.

ECPAT International (2005), "La violencia contra los niños en el ciberespacio". Disponible en el vínculo siguiente: http://www.ecpat.net/EI/Publications/ICT/Cyberspace_SPA.pdf

ESQUIVEL, W. (2010), *Evaluación de resultados intermedios del componente de incidencia política, información y concientización de usuarios del proyecto Derechos y Justicia en el Movimiento social en Internet: la experiencia en Cundinamarca*, Colombia, 2010 (Documento preliminar).

GREGORIO, Carlos *et. al*. (2007), *Documento base del Proyecto Derechos y Justicia en el Movimiento Social en Internet*, IIJusticia, Argentina.

IIJusticia/IDRC (2009), *Memorándum de Montevideo*.

Paniamor/IIJusticia/SCS. (2009), *Expresiones de violencia interpersonal y social desde la perspectiva adolescente: Estado del Arte*, Costa Rica.

Paniamor/IPP-UCR/SCS (2008), *Los usos de las Tecnologías de la Comunicación y la Información en jóvenes de 12 a 18 años del Gran Área Metropolitana*, Costa Rica.

Secretaría de Educación del Departamento de Cundinamarca/Instituto de Investigación para la Justicia (2010), *Protección de la privacidad y datos personales de los niños y adolescentes usuarios de la web: Informe de Resultados*, Colombia.

TERNEUS, A. (2009), *Evaluación externa: apreciaciones sobre el desarrollo del Proyecto Derechos y Justicia y el Movimiento Social en Internet al completar el primer año de ejecución*, Documento Interno, IIJusticia, Argentina.

Programas de prevención y educación para el uso de las redes sociales: la experiencia de Brasil

Rodrigo Nejm[*]

La intensa incorporación de las Tecnologías de la Comunicación e Información (TIC) al cotidiano de niños y adolescentes en las sociedades contemporáneas trae aparejado muchos desafíos a la educación, tanto en el sistema educativo formal como en la formación de la ciudadanía que se da en las familias y espacios públicos de socialización. Sabemos que existe una gran diferencia, en la familiaridad con las TIC entre las generaciones de padres/educadores y de hijos/alumnos. Presenciamos profundos cambios psicosociales en la infancia, la adolescencia y la juventud contemporáneas, cambios producidos por múltiples factores, entre ellos, aunque no solo por ellos, el uso intenso y diverso de las TIC. Seguramente las TIC desempeñan un papel destacado en la transformación del ocio, del estudio, de la forma en comunicar y en jugar de las nuevas generaciones, pero los cambios también son radicales en el marco del universo del consumo, en el conflicto entre generaciones, en el mundo del trabajo, en la conquista de derechos civiles y políticos en algunas sociedades. Como apunta Sonia Livingstone en su reciente libro

[*]El autor es psicólogo, tiene una maestría en Gestión y Desarrollo Social por la Universidad Federal de Bahia/UFBA, y es investigador en el área de psicología y nuevos medios masivos. Actualmente es Director de prevención y asistencia de SaferNet Brasil.

"Children and the Internet" (2009), no podemos centrar la reflexión en las tecnologías sin tener en cuenta otras transformaciones en el mundo del trabajo, de la estructura familiar y del universo del consumo infantil-juvenil.

La incorporación de las TIC en las escuelas y en la dinámica de trabajo de los educadores produjo intensos e interesantes desafíos para la educación. Estos desafíos existen en diferentes áreas y evidencian nuevas demandas para la educación y para el educador dentro y fuera del salón de clases. Los educadores deparan nuevas y urgentes demandas que –muchas veces– los ponen en apuros. Les exigen adaptar sus prácticas incorporando las TIC y otras innovaciones en diferentes aspectos, a modo de ejemplo de demandas inmediatas: la necesidad de los educadores de familiarizarse con el uso de las TIC; la necesidad de remodelación de la didáctica con el uso de las tecnologías en el aula, incorporando Internet a nuevos equipamientos en su práctica pedagógica; urgencia de que comprendan la singularidad de las nuevas formas de relacionarse con la información y con la realidad en las generaciones interactivas; y la necesidad de ampliar el debate de la promoción de la ciudadanía y de los derechos humanos también para las relaciones sociales mediadas por las TIC, cada vez más evidentes e ilustradas por la complejidad del fenómeno de las redes sociales en las cuales millones de niños y adolescentes establecen sus relaciones sociales, construyen vínculos afectivos, se divierten, se informan, consumen y producen contenidos culturales.

En el presente trabajo nos gustaría destacar este último desafío, a partir de la experiencia en Brasil, concentrando nuestra presentación en el compromiso y en el potencial que la escuela y los educadores tienen para contribuir en la promoción del uso ético y responsable de las TIC, principalmente de Internet. Pretendemos enfocar la discusión en la dimensión pública del ciberespacio y del compromiso ético que esta dimensión implica para todos los que se relacionan en el mismo, considerando el desafío de desnaturalizar la noción de que Internet es un espacio sin ley en el cual podemos hacer cualquier cosa con la certeza de la impunidad, como se destaca en 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", producido como fruto de los debates realizados en el "Seminario Derechos, Adolescentes y Redes Sociales en In-

ternet" realizado en Montevideo los días 27 y 28 de julio de 2009:

> 3. Se debe transmitir claramente a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidades. Deben alertarlos para no dejarse engañar con la aparente sensación de que allí todo vale, dado que todas las acciones tienen consecuencias (Memorándum de Montevideo, 2008).

Proponemos esta reflexión a partir de experiencias efectivas de formación de educadores como multiplicadores de la Promoción de los Derechos Humanos en Internet y prevención de los cibercrímenes contra niños y adolescentes en Brasil. Esta experiencia representa un esfuerzo bien logrado de integración de los operadores de derechos, sociedad civil, gestores de los sistemas público y privado de enseñanza dispuestos a sumar esfuerzos en la promoción del uso ético y responsable de las nuevas tecnologías en Brasil. Los talleres de formación de educadores fueron ideados por SaferNet Brasil e implementados a través de la cooperación con Ministerios Públicos Federales, Ministerios Públicos Estaduales, Policía Federal, Secretarías Estaduales y Municipales de Educación en 7 estados diferentes de Brasil. Para sintetizar esta experiencia vamos a presentar brevemente cómo surgió el trabajo y cómo está organizado actualmente, sacando a relucir los datos sobre el uso de Internet y de las redes sociales por parte de niños y adolescentes en Brasil, destacando cómo las acciones educativas pueden consolidar efectivamente una mayor protección de los derechos de niños y adolescentes dentro y fuera del contexto de Internet.

1. SaferNet Brasil y la promoción del uso seguro y responsable de las redes sociales

SaferNet Brasil es una asociación civil sin fines de lucro, sin vinculación político-partidaria, religiosa o racial, fundada el 20 de diciembre de 2005, por un grupo formado por científicos de la computación, profesores universitarios, investigadores y licenciados en Derecho. SaferNet Brasil creó y mantiene la Central Nacional de Denuncias y Crímenes Cibernéticos (litisdenunciación) que, desde el 29 de marzo de 2006, opera en sociedad con el Ministerio Público Federal en Sao Paulo. En noviembre de 2008, firmó un

convenio de cooperación con la Policía Federal y con la Secretaría Especial de Derechos Humanos (SEDH) para fortalecer las acciones de combate a los cibercrímenes contra los Derechos Humanos e integrar la Central con el "Disque 100" (Canal Oficial de denuncia de todo tipo de violencia presencial contra niños y adolescentes en Brasil). La Central de SaferNet ofrece el servicio gratuito y anónimo de recepción, procesamiento, direccionamiento y acompañamiento em línea de denuncias anónimas sobre cualquier crimen o violación a los Derechos Humanos, practicado a través de Internet (racismo, pornografía infantil, apología e incitación a crímenes contra la vida, nazismo, homofobia e intolerancia religiosa).

La importancia de la Central de denuncias puede ser medida por el número de registros que recibe: solo en 2008 SaferNet Brasil recibió más de 90 mil denuncias únicas, siendo más de 57 mil, relacionadas a la pornografía infantil. Más de la mitad de estas denuncias son relativas a contenidos encontrados en redes sociales. En Brasil es sorprendente la adhesión a las redes sociales, inclusive por parte de niños y adolescentes, aún cuando los términos de uso definen 18 años como edad mínima para registro y acceso.

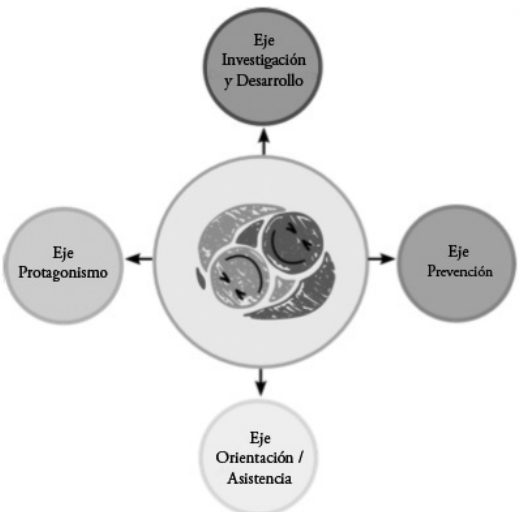
SaferNet ha trabajado para auxiliar a las autoridades a combatir estos crímenes en las redes sociales y otros servicios disponibles en Internet y es cada vez más evidente la intensidad del uso de redes sociales en Brasil. Existen indicadores que marcan que el 75% de los internautas brasileños utilizan la red social de *Google* u *Orkut*.[1] Una investigación de SaferNet realizada en 2008 con niños y adolescentes indicó que 80% de ellos prefieren usar Internet para las redes sociales y 72% para usar los comunicadores instantáneos. Las redes sociales representan la nueva generación de usuarios de Internet, usuarios que pueden crear con mucha más facilidad contenidos y se comunican con costos mínimos. Este uso social de Internet refuerza aún más la necesidad de profundizar también el debate sobre la dimensión humana (y de Derechos Humanos) más allá de la dimensión técnica de Internet. Con la masificación del acceso a Internet y

[1]Artículo en la prensa: 'Orkut: 75% de los internautas brasileños accesan a la red social de Google'. Por Daniela Braun y Evelin Ribeiro el 29 de julio de 2009 en *IDG Now*. Disponible en: http://idgnow.uol.com.br/internet/2009/07/29/orkut-75-dos-internautas-brasileiros-acessam-rede-social-do-google/. Ultimo acceso, 10 de octubre de 2009.

con la convergencia entre las tecnologías, los desafíos incorporados por las redes sociales en términos de seguridad y ética pueden servir de referencia para muchas de las innumerables cuestiones relacionadas al uso (ir)responsable de las TIC y las transformaciones que las misma potencian en las sociedades contemporáneas.

Reconocemos que las acciones de combate a crímenes en Internet deben ser complementadas siempre con actividades educativas y campañas de orientación para evitar que más ciudadanos, especialmente niños y adolescentes, sean víctimas de cibercrímenes. En este sentido, SaferNet Brasil también desarrolla un conjunto de acciones enfocadas en el área de prevención. Considerando que SaferNet Brasil fue la primera organización de la sociedad civil fundada en Brasil para la promoción de los Derechos Humanos en Internet, partiremos de las experiencias ahí desarrolladas para ilustrar parte del escenario brasileño en el ámbito de la promoción del uso seguro de las redes sociales y de Internet en general.

Las acciones de prevención de SaferNet Brasil pueden ser distribuidas a partir de cuatro ejes:



Para movilizar a la sociedad y contribuir con la concientización sobre los Derechos Humanos en línea, los trabajos de los ejes convergen y forman actividades integradas. En el eje 'Investigación y Desarrollo' son realizadas pesquisas con alumnos, educadores y padres sobre los hábitos de navegación en Internet. La investigación permite conocer mejor la realidad local que será abordada, especialmente en lo que respecta a las vulnerabilidades específicas y los tipos de violación a los Derechos Humanos más evidentes en cada contexto. Los datos de las investigaciones nacionales y regionales son tabulados por SaferNet y dirigidos a los socios participantes, con indicaciones de actividades y materiales que puedan satisfacer las necesidades identificadas, ya sea a través de conferencias, talleres y campañas contempladas por los otros ejes. También en este eje se encuentra el desarrollo de tecnologías y materiales que puedan subsidiar las actividades de SaferNet, especialmente en lo que respecta a la producción y adaptación de *softwares* libres, apropiados para trabajar en este tema. SaferNet trabaja fundamentalmente con *softwares* libres y las producciones son licenciadas por Creative Commons para permitir mayor acceso y derechos de uso sobre las informaciones y materiales producidos -por ejemplo las cartillas de las fichas pedagógicas, animaciones, historietas, glosarios, entre otros-.

En el eje 'Protagonismos', buscamos involucrar a niños, adolescentes y jóvenes a evaluar, proponer y orientar la producción no solo de SaferNet, sino también de la política pública en curso sobre el uso de las TIC, especialmente Internet. La participación de estos actores clave, siempre es un reto porque el riesgo de la subordinación a los deseos y las propuestas de los "adultos" siempre está presente cuando no hay incorporación de estas mismas propuestas por los jóvenes que pueden replicar comentarios preformateados para un supuesto papel que acaba siendo sofocado por el discurso hegemónico. Las alternativas que parecen pertinentes para fortalecer la participación de estos actores son: llevar la discusión de los concejos de jóvenes, niños y adolescentes ya movilizados en torno a causas diversas.

En Brasil existen concejos municipales, estaduales y nacionales de jóvenes que se reúnen para discutir los programas y políticas públicas, así como hay una red consolidada de organizaciones de niños y jóvenes que militan por los derechos de los niños, adolescentes y jóvenes. En las actividades de movilización, por ejemplo lo que

sucede durante la semana del Día Mundial de Internet Segura, animamos a estas organizaciones y concejos para crear, a su manera, las oportunidades para la reflexión sobre el tema. En algunas ocasiones se promueven concursos para que los adolescentes y jóvenes puedan demostrar sus habilidades a través del tema propuesto y producir materiales para campañas educativas que se realizan de par a par.

En el marco del eje 'Orientación y Asistencia' consideramos la falta de espacios que sean puntos de apoyo a los internautas donde alguno de sus derechos haya sido violado en Internet. Concentrando nuestros esfuerzos en la orientación de las víctimas de delitos contra los derechos humanos, recibimos muchas demandas de las víctimas de delitos de calumnia, difamación, injuria y falsa identidad. Todo esto expresa cuánto las personas aún no se protegen al interactuar a través de las TIC y no encaran estas interacciones como relaciones que se dan en un espacio público. Los canales de orientación son ofrecidos a través del portal de SaferNet y de correo electrónico, con indicación para los canales que pueden orientar en temas específicos como fraudes bancarios, *spam*, invasión de computadoras o problemas técnicos. Está en desarrollo la versión de comunicador instantáneo que permita ampliar la asistencia a las víctimas y orientación de internautas en relación a los cibercrímenes contra derechos humanos en Brasil.

Finalmente, en el eje 'Prevención' se concentran las actividades directamente vinculadas con las campañas, talleres, conferencias, debates y eventos que son apoyados para diseminar orientaciones necesarias para que podamos disminuir el número de víctimas de cibercrímenes, así como para fortalecer relaciones sociales éticas y responsables también cuando son mediadas por las TIC. En la última parte de este artículo ilustraremos cómo se desarrollan los talleres de movilización de las escuelas y educadores. Los talleres son instancias en las cuales los ejes temáticos son evidentemente integrados para componer una intervención social efectiva, en sintonía con la diversidad de acciones y estrategias ya en curso por otras instituciones, ya sea que ejecuten programas públicos o privados en el área.

Considerando el aún poco explotado potencial de las TIC y especialmente de Internet como fantásticas innovaciones que pueden contribuir valiosamente con el desarrollo cognitivo, social y emocional de nuestros niños, las acciones de prevención de SaferNet Brasil buscan consolidar la dimensión humana de la gran red que to-

davía es interpretada apenas como red de máquinas interconectadas, menospreciando la dimensión de espacio público y de derechos que implica una red de personas. Trabajamos la dimensión pública del ciberespacio, lo que nos obliga a considerar los peligros y amenazas a la seguridad y la salud de niños, jóvenes y adultos como tema de interés público. Algunas visiones fatalistas todavía pregonan a Internet, y dentro de ella especialmente las redes sociales, como villanas de la educación, la moral, la verdadera amistad y la seguridad.

Sin profundizar en detalles y orígenes de estas visiones, nos interesa reforzar la formación de interpretaciones más críticas y constructivas sobre el potencial y los peligros de Internet a través de la promoción y protección de los Derechos Humanos en la misma. El uso de Internet por niños y adolescentes necesita ser estimulado conjuntamente con acciones efectivas de orientación y acompañamiento de padres y educadores, para que el ciberespacio sea interpretado frecuentemente como espacio público que exige respeto a los derechos y compromiso con los deberes que los ciudadanos deben tener en otros espacios sociales. Ciertamente el ciberespacio trae nuevas dimensiones para las relaciones sociales, configurando de esta manera un espacio muy singular con potenciales y amenazas que deben ser actualizados de acuerdo a la inteligencia colectiva que se expresa en la compleja y multifacética cibercultura, como proponen las reflexiones de Pierre Levy (1999).

2. Algunos indicadores de usos y abusos de Internet en Brasil

Brasil representa la quinta mayor población de internautas en el mundo, según datos del *Internet World Stats*, en junio de 2009,[2] con más de 67 millones de usuarios de Internet. Según datos de la investigación de 2008 sobre el uso de las Tecnologías de la Información y Comunicación en Brasil del Comité Gestor de Internet en el país (CGI Br), el 59% de la población brasileña en la franja etárea de 10 a 15 años tuvo acceso a Internet.

[2]Fuente: http://www.internetworldstats.com/stats10.htm, accesado el 15 de octubre de 2009.

En la franja entre 16 y 24 años el porcentaje sube a 69%, siendo que el promedio nacional es de 39% (TIC domicilios 2008)[3]. Cabe destacar que en la franja entre 10 y 15 años, 49% utilizan Internet con más frecuencia en los Centros Públicos Pagos (Lan Houses, Cibercafés), espacios generalmente poco preparados para educar y proteger a niños y adolescentes en relación a los peligros en línea. Todavía en esta franja etárea de 10 a 15 años, 64% emplea entre 1 y 5 horas por semana en Internet y 13% gasta de 6 a 10 horas semanales. En la investigación sobre hábitos de seguridad en línea, realizada por SaferNet en 2008,[4] con 875 niños y adolescentes brasileños, hay indicios de alta vulnerabilidad de este público en Internet.

Del total de los participantes de la investigación, 53% informaron haber tenido contacto con contenidos agresivos y que consideraban impropios para su edad, 28% informaron haberse encontrado personalmente con alguien que conocieron online sin que los padres supieran y 10% informó haber sufrido algún tipo de chantaje online (SaferNet Brasil, 2008). En la misma investigación se evidencia la intensidad del uso de las redes sociales, siendo que entre niños y adolescentes, 79% tienen amigos virtuales y 37% dicen tener más de 20 amigos, 87% dicen que los padres establecen límites para la navegación y 22% afirmaron que "Se sentirían perdidos sin Internet y no imaginan su vida sin ella". La mayoría absoluta de los pequeños internautas brasileños publican con frecuencia información personal como fotos (72%), fecha de cumpleaños (61%), preferencias (69%) y hasta el apellido (51%) en Internet, especialmente a través de las redes sociales que son usadas sin acompañamiento de los padres en 80% de los casos.

Se destaca que en Brasil la red social más utilizada es, teóricamente restricta para menores de 18 años y que el 37% de los participantes de la pesquisa informaron desconocer cualquier programa de prevención de riesgos en línea. Ya en la investigación sobre "Hábitos de Navegación de educadores y alumnos en las escuelas brasileñas" (SaferNet Brasil, 2009), los datos parciales de septiembre de 2009

[3]Fuente: Pesquisa TIC Domicilios 2008, disponible en el vínculo siguiente: http://www.cetic.br/pesquisas/2008/index.htm.

[4]Disponible en el vínculo siguiente: www.safernet.org.br/site/prevencao//pessquias.

indican que entre los alumnos, 19% ha tenido una relación con alguien por Internet al menos 1 vez, 49% recibió o encontró pornografía involuntariamente y 13% ya publicó fotos íntimas en Internet o mensajes de celular (*Sexting*).

Finalmente datos de la investigación "Generaciones Interactivas en Iberoamérica", coordinada por los investigadores Xavier Bringué Sala y Charo Sábada Chalezquer de la Universidad de Navarra (España), realizada con más de 25 mil alumnos en 7 países, nos llama la atención para el lamentable hecho, que Brasil aparece como el país con menor proporción de alumnos que fueron estimulados por sus educadores para usar las TIC. También de esta investigación se desprende la forma individual de uso, el 78% de los adolescentes brasileños acostumbran a utilizar Internet solos, a pesar de que la usan principalmente para interactuar a través de las redes de relacionamiento y comunicadores instantáneos.

Los datos anteriores ilustran cómo los crímenes y violaciones de los derechos tienden a incrementarse progresivamente conforme aumenta el número e intensidad de usuarios de Internet en Brasil, sumando más desafíos al sistema educativo y a los sistemas de garantía de los derechos de los niños y adolescentes en el presente y en el futuro próximo.

El Gobierno Federal Brasileño se ha movilizado para ampliar el acceso de la ciudadanía a las TIC, especialmente Internet. Son más de 20 programas de inclusión digital, ofrecidos por el Gobierno Federal, dentro de los cuales cuatro están directamente vinculados a la educación. Entre ellos podemos destacar el programa "Banda Ancha en las Escuelas", que ya conectó más de 50% de las 56.720 escuelas públicas urbanas del país. Según el último balance realizado por la Agencia Nacional de Telecomunicaciones (ANATEL), cerca de 30 mil escuelas de todo el país ya recibieron Internet de alta velocidad. Hasta fines del año 2009, la expectativa era que 45.381 ya estaban conectadas, lo que corresponde a 80% de todas las escuelas públicas urbanas.

El programa tiene tres frentes de acción. El primero es la instalación de laboratorios de informática, el segundo es la conexión de Internet en banda ancha, que las operadoras llevarán a las escuelas gratuitamente hasta 2025, actualizando la velocidad periódicamente. El tercer frente del programa "Banda Ancha en las Escuelas"

es la capacitación de los docentes. Para ello serán ofrecidos cursos a distancia, que serán acompañados por la Secretaría de Educación a Distancia del Ministerio de Educación. Pese a la complejidad de elaboración y ejecución de programas de esta magnitud, la dimensión de la formación de los educadores todavía es uno de los mayores desafíos, pues el desfase entre el uso de los alumnos y el de los educadores es aún enorme.

Como mencionabamos al comienzo de este artículo, nuestro foco de atención es la promoción del uso seguro y responsable, aplicando las nociones de espacio público y derechos humanos a la interacción con las TIC antes de desarrollar la apropiación pedagógica en la escuela de las mismas. Nos resulta preocupante que la formación sobre riesgo y capacitación de educadores para la prevención de los peligros em línea esté siempre en los últimos lugares en las agendas de formación, generalmente movilizadas después de casos reales de víctimas en el contexto escolar.

La preparación de las familias y de los educadores para la prevención de los peligros en las redes sociales y otros servicios de Internet, debería anteceder a las primeras interacciones con las TIC. Sabemos que esta condición es poco probable teniendo en cuenta el ritmo extremadamente acelerado de las transformaciones sociales y del consumo de tecnologías por las familias, restando a nosotros el desafío de introducir, cuanto antes, este tema en escuelas y familias para ampliar la seguridad en la interacción con las TIC.

3. La formación de educadores como multiplicadores en la promoción del uso ético de las TIC

En las actividades de investigación y formación para educadores y alumnos de escuelas públicas y privadas en diferentes regiones de Brasil, buscamos potenciar el uso seguro y ciudadano de las TIC. El objetivo de los talleres es articular las acciones de combate con las acciones educativas enfocadas en la prevención, proponiendo una aproximación a las TIC por el camino de las relaciones sociales éticas y no obligatoriamente por el enfoque de la pedagogía.

Los talleres para coordinadores pedagógicos y educadores sociales de diferentes instituciones, permiten también fortalecer los

canales de comunicación entre la sociedad civil y las autoridades responsables por la reglamentación y combate de los crímenes cibernéticos, ayudando a consolidar la noción de que Internet no es tierra de nadie. El foco en Internet no opaca las demás tecnologías como la televisión, el celular, los videojuegos y los equipos de música, pues tuvimos en consideración la fuerte convergencia entre estos cuatro, que cada vez más vienen integrados en un mismo equipo. El abaratamiento de los equipos y de los costos de conexión tiende a masificar rápidamente el acceso, lo que no supera las grandes desigualdades en términos de uso de las TIC. Como ya destacaban los análisis sobre las transformaciones sociales intensificadas por las televisión, es necesario desviar el eje del debate de los medios para las mediaciones, "para las articulaciones entre prácticas de comunicación y movimientos sociales, para las diferentes temporalidades y para la pluralidad de matrices culturales" (Barbero, 2001:270) en las que se produce y es negociado el sentido.

De esta forma, SaferNet actúa prestando un servicio de utilidad pública con el objetivo de hacer de la red Internet en Brasil, una puerta segura de entrada a la sociedad de la información para que niños, jóvenes y adultos creen y desarrollen relaciones sociales, éticas, seguras y saludables. De la misma manera que padres y educadores orientan a los niños para determinado cuidado en las calles, la práctica de deportes y su vinculación con extraños en el parque o en la escuela, necesitamos movilizar a la población sobre los cuidados necesarios en cuanto al uso de Internet en casa, en cibercafés, telecentros y celulares. En los talleres "Promoviendo el uso responsable y seguro de Internet", trabajamos para fortalecer el entendimiento de educadores y alumnos sobre el potencial y los beneficios que Internet puede proporcionar a la sociedad, cuando es utilizada con orientación y respeto. Los talleres son realizados a lo largo del año lectivo conjuntamente con instituciones de referencia en cada ciudad, buscando involucrar a los Ministerios Públicos, las Secretarías de Educación, Concejos Tutelares, Foros de Defensa de los Derechos del Niño y Adolescentes y otras instituciones públicas y privadas actuantes en el área.

Para garantizar una educación plena para el uso seguro y ético de Internet en Brasil, es fundamental el compromiso conjunto de los diferentes sectores de la sociedad, especialmente de los proveedores de acceso y servicio, de las empresas publicitarias,

de prensa, de los gestores e instituciones públicas y de las organizaciones de la sociedad civil, todos comprometidos con la promoción de los derechos humanos en todos los espacios. De esta manera podemos luchar con más fuerza para que la red continúe siendo un espacio público libre y abierto para que todos se expresen y se informen en un mundo cada vez más globalizado e interactivo.

Durante los talleres trabajamos temas básicos, junto al material didáctico que es brindado por SaferNet. La intención es que el grupo de participantes regresen como multiplicadores, conociendo bien los materiales para que puedan realizar actividades con sus pares y familiares. Reconociendo la complejidad del tema, SaferNet ofrece a los participantes un espacio interactivo para la aclaración de dudas, búsqueda de nuevos materiales de orientación por Internet. Este espacio está estructurado en una red social propia, en desarrollo y será una forma de mantener un soporte a los participantes, además de representar una importante oportunidad de explicitar la posibilidad concreta de que las redes sociales e Internet, potencien la educación y la ciudadanía cuando son utilizadas de forma orientada y consciente.

La premisa básica de los talleres es mostrar que las relaciones sociales establecidas por medio de las TIC, necesitan ser encaradas como relaciones que se dan en un nuevo espacio público, el ciberespacio. Aún aquellos menos familiarizados con las TIC, pueden tener más facilidad para lidiar con ellas al tener en cuenta los cuidados y aprendizajes aplicados a otros espacios públicos como plazas, calles y parques. Algunos de los encuentros presenciales son transmitidos en vivo a través de videoconferencias y registrados para actividades de réplica en las instituciones representadas en los talleres, dependiendo de la viabilidad técnica de cada grupo local. Los talleres tienen una duración de 4 a 8 horas.

Para que los talleres puedan trabajar con la realidad local de cada ciudad, de cada región y de cada escuela, SaferNet moviliza sus organizaciones fraternas locales para organizar, antes de los talleres, un sondeo sobre hábitos de navegación y vulnerabilidad de alumnos, educadores y padres. La investigación es realizada en línea a través de formularios específicos que están disponibles a través de ligas o *links* y banners desde 2009 (en Paraíba). Este taller fue importante pues en esa ocasión estuvieron presentes y unidos en la temática, organizaciones muy diversas y al mismo tiempo fun-

damentales para contemplar las instituciones educativas públicas y privadas, así como autoridades responsables por la represión de los cibercrímenes, tratando:

– Potencial de Internet y de las redes sociales en Brasil y el mundo.

– Dimensión pública de Internet y la ciberciudadanía.

– Peligros y crímenes en Internet:

– *Ciberbullying* y *Sexting*,

– Seducción sexual por Internet,

– Consejos para mantenerse seguro, y

– Qué pasos seguir en caso de incidentes.

Bajo la coordinación del Procurador de la República Rodolfo Alves, del Ministerio Público Federal de Paraíba, fue posible la firma de acuerdos de cooperación para promoción del uso seguro de Internet con representantes de la Policía Federal Brasileña, Núcleo de Información y Coordinación de Punto BR (organismo que implementa las decisiones y proyectos del Comité Gestor de Internet en Brasil), Ministerio Público Estadual de Paraíba, Secretaría Estadual de Educación de Paraíba, Secretaría Municipal de Educación de la capital João Pessoa, Sindicato de los institutos privados de enseñanza de Paraíba y de instituciones federales de enseñanza.

Para las actividades, la prensa del Estado, se comprometió de forma destacada, ofreciendo espacios en televisión, radio y prensa escrita, para divulgar el evento e invitar a la población a participar. En los dos días de actividades, más de 500 personas participaron de las conferencias, 200 educadores fueron capacitados y 50 autoridades se reunieron para discutir la actualidad en el combate a crímenes contra niños y adolescentes practicados a través de Internet.

Durante los talleres los educadores recibieron material para auxiliarlos en el desarrollo de actividades en el aula de forma transversal a los contenidos curriculares. La propuesta es estimular el debate calificado y orientado sobre los potenciales y riesgos de las redes sociales y del uso de las Tecnologías de la Información y Comunicación. El kit distribuido está compuesto por una cartilla SaferDic@s (consejos seguros), Cartelería de los canales de denuncias y prevención, CD-ROM con historietas glosarios, noticias relacionadas a la tecnología y educación y fichas pedagógicas con sugerencias de actividades para desarrollar en el aula.

4. Consideraciones provisionales

Sabemos que los cambios de hábitos y de comportamientos sociales no se dan de manera inmediata y automática. Seguramente estos cambios ocurren a un ritmo mucho más lento que la evolución e incorporación de nuevas tecnologías en las sociedades contemporáneas. Así como tantos otros procesos educativos, educar para la ciudadanía en línea y para promocionar los Derechos Humanos en el ciberespacio no es tarea sencilla.

En los debates durante los talleres y en las discusiones posteriores hemos escuchado varias sugerencias, críticas y comentarios en general, que apuntan hacia una supuesta crisis de valores que sería expresada por la exposición online de la intimidad, por relaciones de amistad superficiales (más de 300 amigos virtuales), por adhesión masiva a juegos violentos, erotización precoz de la infancia, desapego de las familias en relación a los niños y muchos otros apuntes que demuestran el gran abismo existente entre las generaciones que aún tienen grandes dificultades para comprenderse.

La multiplicidad de lenguajes de Internet componen el imaginario de los internautas de acuerdo a cada contexto. El lugar y la importancia de estos signos en la personalidad dependerán, entre otros, de las circunstancias de recepción y de las relaciones de fuerza que componen el ambiente familiar, escolar y de los propios medios masivos de comunicación. Si antes la familia y la escuela eran los referentes determinantes de la acción y formación de niños y adolescentes, actualmente los medios masivos de comunicación atraviesan todas las instituciones modelando nuevos modos de sociabilidad.

En este contexto, Internet no puede ser pensada como un mero esquema técnico de transmisión de informaciones, pero como parte de un sistema complejo, articulado con todas las instancias socioeconómicas determinantes de las formas de sociabilidad y de

producción de las subjetividades. Estudiando la red de relaciones de los jóvenes internautas vemos que Internet significa un importante espacio de socialización que desencadena relaciones de proyección-identificación e intersubjetividad, participando activamente en la producción de una imagen de sí mismo y de la construcción de la identidad, potenciando la capacidad de comunicación, acceso y distribución de información sobre sí mismo y sobre sus pares de una manera nunca antes posible.

Los educadores necesitan adecuarse, no apenas a los equipamientos en las escuelas, sino también comprender la dinámica de interacción que las nuevas generaciones de alumnos establecen con la información y con las instituciones sociales. Frente a esta compleja situación nos preguntamos cuán importante es avanzar en la apropiación del propio ciberespacio para promover orientaciones que permitan amparar a las víctimas y prevenir a jóvenes internautas acerca de los peligros *online*.

Las TIC no son en sí mismas responsables por los nuevos peligros, pero podemos arriesgarnos a decir que ellas potencian las más diversas transformaciones sociales, así como potencian la capacidad de expresión del imaginario y de las fantasías que materializan nuevos comportamientos. Lo que nos parece emblemático es el desafío de lograr usufructuar de las propias TIC para fortalecer acciones educativas y potenciar el uso ético, no apenas de los equipamientos, sino también el comportamiento ético en las relaciones sociales, mediadas o no por las TIC. Sin dudas las TIC continuarán siendo incorporadas, cada vez más tempranamente, por todo tipo de personas de diversas regiones, restando a nosotros sumar esfuerzos para que este proceso pueda darse en sintonía con los movimientos que buscan consolidar una sociedad cada vez más justa y pacífica, también en este nuevo espacio público global, viabilizado por las redes sociales.

Referencias Bibliográficas

BIRMAN, J. (1999), *Mal-estar na atualidade: a psicanálise e as novas formas de subjetivação*, Civilização Brasileira, Rio de Janeiro.

CASTELLS, M. (1999), "A sociedade em rede. A era da informação: economia, sociedade e cultura", Vol. 1., *Paz e Terra*, Sao Paulo.

DEBORD, Guy (1997), *A sociedade do espetáculo*, Contraponto, Rio de Janeiro.

DELEUZE, G. y F. GUATARRI (1995), *Mil Platôs*, vol. 1 y 2, Ed. 34, Rio de Janeiro.

GARCÍA, C. Néstor (2000), *Culturas Híbridas*, EDUSP, Sao Paulo.

IANNI, Octavio (2000), *Enigmas da Modernidade – Mundo, Civilização* Brasileira, Rio de Janeiro.

LEVY, P. (1993), *Inteligência coletiva*, Ed. 34, Rio de Janeiro.

—— (1999), *Cibercultura*, Ed. 34, Sao Paulo.

LIVINGSTONE, S. (2009), *Children and Internet: Great Expectations, Challenging Realities*, Polity, Cambridge.

MARCONDES, C. (coord.) (1996), *Pensar-Pulsar: cultura comunicacional, tecnologias, velocidade*, Coletivo NTC, Sao Paulo.

MARTÍN-BARBERO, J. (2001), *Dos meios às mediações*, Ed. UFRJ, Rio de Janeiro.

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet en particular de niños, niñas y adolescentes. Seminario Derechos, Adolescentes y Redes Sociales en Internet, Montevideo, Uruguay 27 y 28 de julio de 2009.

PARENTE, A.(1993), *Imagem-Máquina: A era das tecnologias do virtual*, Ed. 34, Rio de Janeiro.

SALA, X.B. y C.S. CHALEZQUER (coords.) (2008), *Gerações Interativas na Ibero-América: crianças e adolescentes diante das telas*, Fundação telefônica, Ariel, España.

Apéndice Documental

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes

Memorándum de Montevideo[*]

1. Consideraciones generales

La Sociedad de la Información y el Conocimiento, con herramientas como Internet y las redes sociales digitales, es una oportunidad inestimable para el acceso e intercambio de información, propagación de ideas, participación ciudadana, diversión e integración social, especialmente a través de las redes sociales.

Los niños, niñas y adolescentes tienen cada vez mayor acceso a los distintos sistemas de comunicación, que les permiten obtener todos los beneficios que ellos representan, pero esta situación también ha llevado al límite el balance entre el ejercicio de los derechos fundamentales y los riesgos —para la vida privada, el honor, buen nombre, y la intimidad, entre otros— que, así como los abusos de los cuales pueden ser víctimas —como discriminación, explotación sexual, pornografía, entre otros— pueden tener un impacto negativo en su desarrollo integral y vida adulta.

En América Latina y el Caribe, así como en otras regiones, se están realizando esfuerzos, dentro de la diversidad social, cultural,

[*]Recomendaciones adoptadas en el *Seminario Derechos, Adolescentes y Redes Sociales en Internet* (con la participación de: Belén Albornoz, Florencia Barindelli, Chantal Bernier, Miguel Cilleron, José Clastornik, Rosario Duaso, Carlos G. Gregorio, Esther Mitjans, Federico Moteverde, Erick Iriarte, Thiago Tavares Nunces de Oliveira, Lina Ornelas, Leila Regina Paiva de Souza, Ricardo Pérez Manrique, Nelson Remolina, Farith Simon y María José Viega) realizado en Montevideo los días 27 y 28 de Julio de 2009.

política y normativa existente, para lograr consenso y racionalidad de modo tal de establecer un equilibrio entre la garantía de los derechos y la protección ante los riesgos en la Sociedad de la Información y el Conocimiento. En ese sentido, podemos citar, entre otros, los más recientes documentos: el *Acordo que põe fim à disputa judicial entre o Ministerio Público Federal de Brasil e a Google* (del 1 de julio de 2008);[1] *la Child Online Protection Initiative* de la Unión Internacional de Telecomunicaciones (del 18 de mayo de 2009);[2] la *Opinion 5/2009 on online social networking,* del Grupo Europeo de Trabajo del Artículo 29 (del 12 de Junio de 2009);[3] el *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. / Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc.*[4] (del 16 de julio de 2009).[5]

Las recomendaciones que se presentan a continuación son una contribución para que los diversos actores involucrados de la región se comprometan con el tema para extender los aspectos positivos de la Sociedad de la Información y Conocimiento, incluyendo Internet y las redes sociales digitales, así como prevenir aquellas prácticas perjudiciales que serán muy difíciles de revertir, así como los impactos negativos que las mismas conllevan.

Cualquier acercamiento al tema requiere que se consideren dos dimensiones. Por un lado el reconocimiento que niñas, niños y adolescentes son titulares de todos los derechos, y por tanto pueden ejercerlos en función de su edad y madurez, además que sus opiniones deben ser consideradas en función de sus edad y madurez, por otro, el hecho de que por su particular condición de desarrollo tienen el derecho a una protección especial en aquellas situaciones que pueden resultar perjudiciales para su desarrollo y derechos.

[1] http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/

[2] http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html

[3] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

[4] http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

[5] Otros documentos especialmente considerados: *Strasbourg's Resolution on Privacy Protection in Social Network Services* (17 de octubre de 2008); "Recomendación sobre redes sociales" de la Agencia Española de Protección de Datos, "Estudio sobre la privacidad de los datos personales y privacidad y la seguridad de la información en las Redes Sociales on line" , realizado por el Instituto Nacional de Tecnologías de la Comunicación, INTECO y por la Agencia Española de Protección de Datos (2009), *The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents* (noviembre 2008), el Dictamen 2/2009 sobre la protección de los datos personales de los niños del Grupo Europeo de Trabajo del Artículo 29 (2009); el Informe de Análisis y Propuestas en materia de Acceso a la Información y Privacidad en América Latina del Monitor de Privacidad y Acceso a la Información, y los documentos de eLAC 2007 y 2010.

El derecho a la vida privada es un valor que toda sociedad democrática debe respetar. Por tanto para asegurar la autonomía de los individuos para decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer intromisiones ilegales o arbitrarias, en dicha esfera personal. En particular debe protegerse la información personal de niñas, niños y adolescentes sin que se afecte su dignidad como personas ya que ellos tienen una expectativa razonable de privacidad al compartir su información en ambientes digitales, dado que consideran que se encuentran en un espacio privado.

En este sentido, se recuerda la importancia de que las niñas, niños y adolescentes sean consultados y sus opiniones sean tomadas en cuenta en las medidas que se implementen en esta materia.

La sociedad civil espera de los agentes económicos la declaración de adhesión a principios, actitudes y procedimientos que garanticen los derechos de los niños, niñas y adolescentes en la Sociedad de la Información y el Conocimiento.

En lo que refiere a la erradicación de la pornografía infantil en Internet, se espera un esfuerzo conjunto de todos los actores responsables —gobiernos, policía, proveedores de acceso y de contenidos, sociedad civil, sector privado— en el plano nacional, regional e internacional, para movilizar e involucrar un número cada vez mayor de empresas, organizaciones públicas y de la sociedad civil.

Para estas recomendaciones se han tenido en cuenta las particularidades de género y la diversidad cultural que se presenta en América Latina y el Caribe, así como la variedad de políticas y de normativas en la manera de enfrentarse al fenómeno de la Sociedad de la Información y el Conocimiento, con especial énfasis en Internet y las redes sociales digitales.

Los organismos multilaterales deberán incluir en sus docu-

mentos, directrices o recomendaciones a las niñas, niños y adolescentes, como sujetos especialmente protegidos y vulnerables respecto del tratamiento de sus datos personales. Asimismo deberán enfocar esfuerzos para promover o fortalecer una cultura de protección de datos en las niñas, niños y adolescentes.

Las presentes recomendaciones utilizan como referente normativo fundamental la Convención de Naciones Unidas sobre los Derechos del Niño (CDN), instrumento ratificado por todos los países de la región, en el que se reconoce claramente la responsabilidad compartida dentro de sus ámbitos respectivos, de la sociedad y el Estado, en la protección de la infancia y la adolescencia. Esto a partir de tres consideraciones fundamentales: el reconocimiento del papel relevante que cumple la familia, o quien se encuentre del cuidado de las niñas, niños y adolescentes en el proceso de educación sobre el uso responsable y seguro de herramientas como Internet y las redes sociales digitales y en la protección y garantía de sus derechos; la necesidad de que todas las medidas que se tomen prioricen el interés superior de niñas, niños y adolescentes, guardando un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de esas herramientas que representan formas de ejercicio de sus derechos; y, que todo aquel que se beneficie de cualquier forma de Internet y de las redes sociales digitales son responsables por los servicios que proveen y por tanto deben asumir su responsabilidad en las soluciones a la problemática que se genera.

2. Recomendaciones para los Estados y entidades educativas para la prevención y educación de niñas, niños y adolescentes

Toda acción en materia de protección de los datos personales y vida privada de las niñas, niños y adolescentes[6] debe considerar

[6]Las expresiones niña, niño y adolescente se usan con el sentido que en cada país les da la legislación nacional. (según el país las expresiones niña o niño podrán referirse a las personas que no han cumplido los 12 o 13 años de edad, y adolescente a quienes son mayores de esa edad y menores de 18 años. En aquellos países en los que no se ha introducido jurídicamente la categoría "adolescentes" se aplica a los llamados "menores adultos" o "menores púberes". En el caso de Honduras niño es la persona menor de 14 años y niña es la persona menor de 12 años, adolescentes son los mayores de esas edades y menores de 18 años).

el principio del interés superior[7] y el artículo 16 de la CDN que determina que:

> "(1). Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia ni de ataques ilegales a su honra y a su reputación. (2). El niño tiene derecho a la protección de la ley contra esas injerencias o ataques".

Es prioritaria la prevención, —sin dejar de lado un enfoque de políticas, normativo y judicial— para enfrentar los aspectos identificados como riesgosos de la Sociedad de la Información y Conocimiento, en especial del Internet y las redes sociales digitales, fundamentalmente por medio de la educación, considerando la participación activa de los propios niños, niñas y adolescentes, los progenitores u otras personas a cargo de su cuidado y los educadores, tomando en consideración como principio fundamental el interés superior de niñas, niños y adolescentes.

Para esto se debe tomar en consideración las siguientes recomendaciones:

1. Los Estados y las entidades educativas deben tener en cuenta el rol de los progenitores, o cualquier otra persona que tenga bajo su responsabilidad el cuidado de las niñas, niños y adolescentes, en la formación personal de ellos, que incluye el uso responsable y seguro del Internet y las redes sociales digitales. Es tarea del Estado y las entidades educativas proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales.

2. Toda medida que implique control de las comunicaciones tiene que respetar el principio de proporcionalidad por tanto se debe determinar que la misma tiene como fin la protección y garantía de derechos que es adecuada al fin perseguido y que no existe otra medida que permite obtener los mismos resultados y sea menos restrictiva de los derechos.

[7]El artículo 3.1 de la CDN establece lo siguiente: "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".

3. Se debe transmitir claramente a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidades. Deben alertarlos para no dejarse engañar con la aparente sensación de que allí todo vale dado que todas las acciones tienen consecuencias.

Deben ser educados en el uso responsable y seguro de Internet y las redes sociales digitales. En particular:

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 identidad 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.

3.2. En el proceso educativo es necesario enfatizar el respeto a la vida privada, intimidad y buen nombre de terceras personas, entre otros temas. Es importante que las niñas, niños y adolescentes sepan que aquello que puedan divulgar puede vulnerar sus derechos y los de terceros.

3.3. Los niños, niñas y adolescentes deben conocer que la distribución de contenidos prohibidos por la regulación local y regional (en especial la pornografía infantil), el acoso (en especial el acoso sexual), la discriminación, la promoción del odio racial, la difamación, la violencia, entre otros, son ilegales en Internet y en las redes sociales digitales y están penados por la ley.

3.4. El proceso educativo debe proveer de conocimiento acerca del uso responsable y seguro por parte de las niñas, niños y adolescentes de las políticas de privacidad, seguridad y alertas con las que cuentan los instrumentos de acceso y aquellos sitios web en los que las niñas, niños y adolescentes son usuarios frecuentes como las redes sociales digitales.

3.5. Se debe promover una política educativa —expresada en

términos acordes a la edad de las niñas, niños y adolescentes — que incluya una estrategia informativa y formativa que los ayude a gestionar las potencialidades y los riesgos derivados de la Sociedad de Información y el Conocimiento, en especial del uso de Internet y de las redes sociales digitales.

3.6. Asimismo se debe informar sobre los mecanismos de protección y las responsabilidades civiles, penales o administrativas que existen cuando se vulneran derechos propios o de terceros en la red.

3.7. Se debe advertir del peligro que supone el llamado robo y/o suplantación de identidad que se puede producir en los entornos digitales que inducen al engaño.

3.8. Es necesario explicar a las niñas, niños y adolescentes con un lenguaje de fácil comprensión el espíritu de las leyes sobre protección de datos personales y protección de la vida privada de modo tal que puedan captar la idea de la importancia del respeto a la privacidad de las informaciones personales de cada uno de ellos y de los demás.

3.9. Es necesario educar para la incertidumbre sobre la veracidad de los contenidos y la validación de las fuentes de información. Se debe enseñar a las niñas, niños y adolescentes a buscar y a discriminar las fuentes.

4. Se recomienda enfáticamente la promoción de una sostenida y completa educación sobre la Sociedad de la Información y el Conocimiento, en especial para el uso responsable y seguro del Internet y las redes sociales digitales, particularmente por medio de:

4.1. La inclusión en los planes de estudios, a todos los niveles educativos, de información básica sobre la importancia de la vida privada y de la protección de los datos personales, y demás aspectos indicados en numeral tres.

4.2. La producción de material didáctico, especialmente audiovisuales, páginas web y herramientas interactivas (tales como juegos *online*) en el que se presenten los potencialidades y los riesgos. Estos materiales deberán incluir información acerca de los mecanismos de protección de los derechos.

La naturaleza de estos temas y materiales exige de la participación y discusión de los mismos por parte de todos los ac-

tores involucrados y con ello responder a las particularidades locales y culturales.[8]

4.3. Los docentes deben ser capacitados para facilitar la discusión y poner en contexto las ventajas y los riesgos de la Sociedad de la Información y el Conocimiento, y en especial de Internet y las redes sociales digitales; pudiendo contar para ello con el apoyo de las autoridades de protección de los datos personales o de todas aquellas organizaciones que trabajen en este tema en los diferentes países.

4.4. Las autoridades educativas —con el apoyo de las autoridades de protección de datos (donde existan), el sector académico, las organizaciones de la sociedad civil, el sector privado y, cuando sea necesario, con la cooperación internacional— deben asistir a los docentes y apoyar el trabajo en las áreas descritas.

5. Las autoridades competentes deben establecer mecanismos para que los centros educativos resuelvan los conflictos, que se generen como consecuencia del uso de Internet y las redes sociales digitales por parte de las niñas, niños y adolescentes, con un sentido didáctico, siempre considerando el interés superior de los mismos, sin vulnerar derechos y garantías, en particular el derecho a la educación.

3. Recomendaciones para los Estados sobre el marco legal

El marco legal que regula la Sociedad de la Información y Conocimiento en la región —en particular Internet y las redes sociales digitales— avanza lentamente en comparación con el desarrollo de nuevas aplicaciones y contenidos, tiene una serie de

[8] *ITU Guidelines for Policy Makers*, Checklist 3) y 4): " … It is very important, therefore, that materials are produced locally which reflect local laws as well as local cultural norms. This will be essential for any Internet safety campaign or any training materials that are developed."; 4. " … When producing educational materials it is important to bear in mind that many people who are new to the technology will not feel comfortable using it. For that reason it is important to ensure that safety materials are made available in either written form or produced using other media with which newcomers will feel more familiar, for example, with video".

vacíos y contiene tensiones importantes en los valores que le inspira y en la forma de proteger los distintos derechos. No obstante existe algún nivel de consenso en que existen suficientes principios fundamentales y constitucionales para iluminar las decisiones que se tomen en la materia.

La creación, reforma o armonización normativa deben hacerse tomando como consideración primordial el interés superior de niñas, niños y adolescentes , especialmente debe considerarse lo siguiente:

6. La protección de los datos personales requiere del desarrollo de una normativa nacional, aplicable al sector público y privado, que contenga los derechos y principios básicos, reconocidos internacionalmente, y los mecanismos para la aplicación efectiva de la misma. Los Estados deberán tomar en especial consideración, en la creación y en el desarrollo de dichas normativas, a las niñas, niños y adolescentes.

7. Debe asegurarse que cualquier acción u omisión contra una niña, niño o adolescente considerado ilegal en el mundo real tenga el mismo tratamiento en el mundo virtual, siempre garantizando su bienestar y la protección integral a sus derechos.[9]

8. Los Estados deben legislar el derecho que tienen las niñas, niños y adolescentes directamente o por medio de sus representantes legales, a solicitar el acceso a la información que sobre sí mismos se encuentra en bases de datos tanto públicas como privadas, a la rectificación o cancelación de dicha información cuando resulte procedente, así como a la oposición a su uso para cualquier fin.

9. Debe desarrollarse una adecuada regulación para el funcionamiento de los centros de acceso a Internet (públicos o privados) que puede incluir, por ejemplo, la obligación de utilizar mensajes de advertencia, filtros de contenido, accesibilidad para las niñas, niños y adolescentes, etc.

[9] *ITU Guidelines for Policy Makers*, Checklist 2): "Establish, mutatis mutandis, that any act against a child which is illegal in the real world is illegal online and that the online data protection and privacy rules for legal minors are also adequate".

4. Recomendaciones para la aplicación de las leyes por parte de los Estados

En años recientes muchos conflictos o violaciones de derechos como consecuencia de difusión de datos personales, invasión de la vida privada, difamaciones en Internet y las redes sociales digitales han llegado a los Tribunales de Justicia. Algunas decisiones han mostrado el rol de los jueces para decidir situaciones nuevas con apego a los principios fundamentales. Sin embargo la proporción de conflictos que tienen un real acceso a la justicia es mínima.

Los sistemas judiciales tienen un rol muy relevante en el aseguramiento de un buen uso de Internet y las redes sociales digitales. Las sanciones civiles y penales deben aplicarse no solo para rectificar los derechos vulnerados sino también para enviar a los ciudadanos y a las empresas reglas claras sobre la interpretación de las leyes y de los principios fundamentales.[10]

10. Se debe garantizar:

10.1. Que existan procesos judiciales y administrativos sencillos, ágiles, de fácil acceso y que sea tramitados con prioridad por parte de los tribunales y autoridades responsables.[11]

Se debe fortalecer el uso de la responsabilidad civil extracontractual objetiva como mecanismo regulatorio para garantizar los derechos fundamentales en las aplicaciones en la Sociedad de la Información y Conocimiento, Internet y redes sociales digitales. Las sanciones judiciales por los daños derivados tienen la ventaja de ser una respuesta inmediata, eficiente y capaz de desincentivar los diseños peligrosos. Este

[10] *Declaración de Principios sobre Libertad de Expresión*, de la Comisión Interamericana de Derechos Humanos de la O.E.A. (Octubre de 2000): "10. Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas". [Aprobada durante el 108° Período Ordinario de Sesiones de la CIDH].

[11] En este sentido se destaca la intervención de los *Juizados Especiais* de Brasil en la protección de los derechos de los ciudadanos en las redes sociales en Internet.

tipo de responsabilidad civil se fundamenta en el interés superior del niño.

10.2. Las decisiones que se tomen en esta materia deberían tener la más amplia difusión posible, utilizando técnicas de anonimización que garanticen la protección de datos personales.

10.3. Debería desarrollarse y difundirse una base de datos sobre casos y decisiones (fallos judiciales o resoluciones administrativas anonimizadas) vinculada a la Sociedad de la Información y el Conocimiento, en especial a Internet y las redes sociales digitales, que sería un instrumento para que los jueces puedan apreciar el contexto nacional e internacional en el que están decidiendo.

11. Se debe establecer un canal de comunicación que permita a los niños, niñas y adolescentes presentar las denuncias que puedan surgir por la vulneración de sus derechos, en materia de protección de datos personales.

12. Fomentar el establecimiento de organismos jurisdiccionales especializados en materia de protección de datos.

13. Desarrollar capacidades en los actores jurídicos involucrados en materia de protección de datos, con especial énfasis en la protección de niñas, niños y adolescentes.

5. Recomendaciones en materia de políticas públicas

Recordamos la necesidad de que el interés superior del niño sea considerado como principio rector de toda medida que se tome en la materia, particularmente en el desarrollo de políticas públicas tendientes a regular las redes sociales digitales.[12]

14. Se recomienda considerar la implementación de las siguientes políticas públicas:

[12] *Opinion 5:* 4. "The Opinion emphasized the need for taking into account the best interest of the child as also set out in the UN Convention on the Rights of the Child. The Working Party wishes to stress the importance of this principle also in the context of SNS".

14.1 Establecimiento de mecanismos de respuesta para atención a las víctimas de abusos en la Sociedad de la Información y el Conocimiento, en especial en Internet o en las redes sociales digitales. De igual manera se debe establecer sistemas de información para que, aquellas niñas, niños y adolescentes que tengan alguna preocupación por los contenidos en Internet o las redes sociales digitales, puedan tener asesoría y apoyo rápido.

Para esto se pueden generar medidas como ayuda y denuncia en línea, números gratuitos telefónicos, centros de atención, etc.

14.2. Elaboración de protocolos para canalizar los contenidos ilegales reportados.[13]

15. Deberían existir mecanismos regionales e internacionales para compartir la información reportada por particulares sobre estos eventos, en tiempo real, para poder así generar políticas y mecanismos de protección en forma temprana, esto debido a que los riesgos que se generan en las redes sociales digitales están muy dispersos y nos son plenamente advertidos.

16. Promover acciones de sensibilización y divulgación de información a través de los medios de prensa y de comunicación masiva y las propias redes sociales, entre otros, porque son un vehículo efectivo para fomentar un uso responsable y seguro de las herramientas de la Sociedad de Información y el Conocimiento.[14]

17. Promover el compromiso y la participación de las asociaciones públicas y privadas, así como redes nacionales de centros de acceso a Internet (donde hubiere), para asegurar su participación en la protección y en las campañas de alerta sobre las potencialidades y los riesgos de Internet y las redes sociales digitales.

[13] *ITU Guidelines for Policy Makers*, Checklist 5), 6) y 7): "5. Consider taking additional measures to disrupt or reduce the traffic in CAM, for example by establishing a national hotline and by deploying measures which will block access to web sites and Usenet Newsgroups known to contain or advertise the availability of CAM. 6. Ensure that a mechanism is established and is widely promoted to provide a readily understood means for reporting illegal content found on the Internet, for example, a national hotline which has the capacity to respond rapidly and have illegal material removed or rendered inaccessible. 7. Ensure that national processes are in place which ensure that all CAM found in a country is channelled towards a centralised, national resource. One example is the National Child Abuse Material Management Centre".

[14] *ITU Guidelines for Policy Makers*, Checklist 2): "Consideration should also be given to enlisting the aid of the mass media in promoting awareness messages and campaigns".

18. Impulsar la generación de conocimiento especializado con el fin de elaborar políticas públicas adecuadas. En especial, en lo que refiere a los comportamientos en línea de niñas, niños y adolescentes, se sugiere investigar acerca de los roles que estos juegan en la recepción, producción, almacenamiento y reproducción de contenidos ilegales, las medidas de protección que ellos mismos desarrollan, las motivaciones individuales y colectivas de dichos comportamientos, así como los peligros reales a los que se enfrentan en la Sociedad de la Información y el Conocimiento.

6. Recomendaciones para la industria

Las empresas que proveen los servicios de acceso a Internet, desarrollan las aplicaciones o las redes sociales digitales deben comprometerse de manera decidida en materia de protección de datos personales y la vida privada —en particular de niñas, niños y adolescentes—, a cooperar con los sistemas de justicia nacionales, desarrollar campañas de prevención y desarrollo de capacidades, entre otros instrumentos mediante compromisos o códigos de conducta, que deben incluir:

19. No permitir la recopilación, tratamiento, difusión, publicación o transmisión a terceros de datos personales, sin el consentimiento explícito de la persona concernida. Se debe restringir el uso de la información recogida con cualquier otra finalidad diferente a la que motivó su tratamiento, y en especial a la creación de perfiles de comportamiento.[15]

En el caso de niñas y niños se deberá considerar la prohibición de tratamiento de datos personales. En el caso de adolescentes se

[15] *Opinion 5:* 3.4. "Sensitive personal data may only be published on the Internet with the explicit consent from the data subject or if the data subject has made the data manifestly public himself".

deberá tener en cuenta los mecanismos de controles parentales de acuerdo a la legislación de cada país, de los que deben darse una información clara.

20. Proteger la vida privada debería ser la característica general y por defecto en todas las redes sociales digitales, bases de datos y sistemas de comunicación, entre otros. Los cambios en el grado de privacidad de su perfil de usuario que se quieran realizar deben ser sencillos y sin costo alguno.

21. Las reglas sobre privacidad de las páginas web, servicios, aplicaciones, entre otros, deberían ser explícitas, sencillas y claras, explicadas en un lenguaje adecuado para niñas, niños y adolescentes.

Se deberá proveer información sobre los propósitos y finalidades para los cuales se utilizarán los datos personales, así como las transmisiones que se realicen a terceros. De igual modo se deberá indicar la persona o personas responsables del tratamiento de la información.

Se debe igualmente ofrecer un enlace hacia los "parámetros de privacidad" en el momento de la inscripción, conteniendo una explicación clara sobre el objeto de dichos parámetros.

Debe hacerse accesible igualmente un aviso sobre el hecho de que la red social ha preseleccionado los parámetros, si éste es el caso, y que pueden ser cambiados en todo momento, según las preferencias de las niñas, niños y adolescentes.

Sería deseable igualmente que se cambien los "parámetros por defecto" de los contenidos personales, para que puedan ser únicamente accesibles por los amigos y las redes que el usuario determine.[16]

22. Toda red social digital debe indicar explícitamente en la parte relativa a la "publicidad" contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean

[16] *Office of the Privacy Commissioner of Canada*, PIPEDA Case Summary 2009-008, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act", 16 de julio de 2009.

para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.[17]

23. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital.

Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria.[18]

La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.

24. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley.[19]

Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable. Asimismo se deberá eliminar la información de no usuarios, considerando un límite razonable de conservación cuando han sido invitados a ser parte de las redes. Las redes sociales digitales no deben utilizar la información de no usuarios.

Las dos opciones que permitan desactivar y suprimir las cuentas deben ser totalmente visibles para los usuarios, que deben poder comprender qué supone cada opción en cuanto a la gestión por parte del servicio de los datos contenidos en dichas cuentas.[20]

[17] *Ibid.*

[18] *Ibid.*

[19] El espíritu de este último párrafo es no excluir —por el tiempo que sea necesaria— la retención de los datos de los usuarios que puedan ser necesarios en la investigación de delitos.

[20] *Office of the Privacy Commissioner of Canada*, PIPEDA Case Summary 2009-008,

Se tiene que informar a los usuarios de las obligaciones de privacidad frente a terceros, dicha política debe ser explícita, clara y visible.

25. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos.

26. Toda red social digital debe establecer las medidas necesarias para limitar el acceso por parte de los terceros que desarrollan las diferentes aplicaciones que el servicio ofrece (juegos, cuestionarios, anuncios, entre otros), a los datos personales de los usuarios cuando éstos no sean necesarios ni pertinentes para el funcionamiento de dichas aplicaciones.

La red social tiene que asegurar que los terceros que desarrollan aplicaciones en sus plataformas únicamente podrán acceder a los datos personales de los usuarios con el consentimiento expreso de estos. La red social digital debe asegurarse que los terceros desarrolladores soliciten únicamente la información indispensable, pertinente y no excesiva para el uso de dicha aplicación.

Es igualmente importante que se tomen las medidas necesarias para evitar toda comunicación de datos personales de aquellos usuarios que no han decidido expresamente por ellos mismos el instalar alguna aplicación.[21]

27. Estas recomendaciones se aplican al tratamiento de los datos personales en las redes sociales digitales aunque sus domicilios legales estén fuera de América Latina y el Caribe. Para facilitar el acceso a la justicia de los usuarios, cada empresa proveedora de redes sociales digitales debe fijar un domicilio o representante legal en los

"Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act", 16 de julio de 2009.

[21] *Office of the Privacy Commissioner of Canada*, PIPEDA Case Summary 2009-008, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act", 16 de julio de 2009.

países en los que esa red social tiene un uso significativo o a requisitoria del Estado.

Las redes sociales digitales deberán establecer un servicio eficiente y eficaz de soporte a los usuarios en estos temas. Este soporte deberá ser en las lenguas oficiales utilizadas en el país del usuario.

28. Los desarrolladores de páginas web, servicios, aplicaciones, plataformas, entre otros, deberán establecer filtros de seguridad, como medio complementario a la educación, sensibilización y sanción.[22]

29 La industria debe establecer medidas de índole técnica y operativa para garantizar la seguridad de la información, en particular la integridad, disponibilidad y confidencialidad.

30. Para la erradicación de la pornografía infantil en Internet la industria —en un esfuerzo conjunto de todos los actores responsables– deben comprometerse como mínimo a:

30.1. Notificar a las autoridades competentes todas las ocurrencias de pornografía infantil detectadas en perfiles de los usuarios de redes sociales digitales, para que sea posible abrir las investigaciones y acciones que correspondan;

30.2. Preservar todos los datos necesarios para la investigación por el plazo mínimo de seis meses o entregar esos datos a las autoridades competentes, mediando autorización judicial;

30.3. Preservar los contenidos publicados por usuarios los usuarios de las redes sociales por el mismo plazo, y entregar esos contenidos a las autoridades públicas mediando autorización judicial;

30.4. Cumplir integralmente las legislaciones nacionales en relación con los crímenes cibernéticos practicados por los ciudadanos de los respectivos países de América Latina y el Caribe o por medio de conexiones a Internet realizadas desde las respectivas jurisdicciones nacionales;

[22] *ITU Guidelines for Policy Makers*, Checklist 13): "Consider the role that technical tools such as filtering programmes and child safety software can play in supporting and supplementing education and awareness initiatives".

30.5. Reformular el servicio de atención a clientes y usuarios para dar una respuesta en un tiempo razonable a todas las reclamaciones formuladas por correo electrónico o por vía postal por las personas perjudicadas por la creación de comunidades falsas u ofensivas;

30.6. Desarrollar una tecnología eficiente de filtrado e implementación de moderación humana para impedir la publicación de fotografías e imágenes de pornografía infantil en el servicio de las redes sociales digitales;

30.7. Desarrollar herramientas por medio de las cuales las líneas telefónicas de ayuda a niñas, niños y adolescentes puedan encaminar las denuncias para que los funcionarios de la empresa analicen, retiren los contenidos ilegales e informen a las autoridades competentes cuando contengan indicios de pornografía infantil, racismo u otros crímenes de odio, y preserven todas las pruebas;

30.8. Retirar los contenidos ilícitos, ya sea mediante orden judicial, o por requerimiento de autoridad pública competente, preservando los datos necesarios para la identificación de los autores de esos contenidos;

30.9. Desarrollar herramientas de comunicación con las autoridades competentes, para facilitar la tramitación de las denuncias, formulación de pedidos de remoción y preservación de datos;

30.10. Informar adecuadamente a los usuarios nacionales sobre los principales delitos cometidos en las redes sociales digitales (pornografía infantil, crímenes de odio, delitos contra la honra, entre otros);

30.11. Desarrollar campañas de educación para el uso seguro y respetuoso de las leyes, de Internet y las redes sociales digitales;

30.12. Financiar la publicación de folletos y su distribución a niñas, niños y adolescentes en escuelas públicas, con información para el uso seguro de Internet y las redes sociales;

30.13. Mantener un enlace en los sitios de las redes sociales

digitales con sitios de denuncia o líneas de ayuda a niñas, niños y adolescentes.

7. Consideraciones finales

31. Las recomendaciones señaladas para niñas, niños y adolescentes se extiendan a otras personas (mayores de edad) que en razón de su condición personal se encuentre en una posición de vulnerabilidad.

Se entienden por grupos vulnerables todos aquellos relacionados a los datos sensibles (según cada una de las legislaciones nacionales) que generalmente incluyen trabajadores, disidentes, personas con discapacidad y sus familias, inmigrantes y emigrantes, entre otros.

32. Se exhorta a todos los actores involucrados a discutir e interpretar las presentes recomendaciones. De igual modo se debe buscar un diálogo constante en esta materia a la luz del presente documento. De manera especial se apela al cumplimento de las obligaciones de los Estados y a la responsabilidad social empresarial para encontrar las mejores formas de implementar el presente documento.

Montevideo, 28 de julio de 2009

Recomendaciones adoptadas en el Seminario Derechos, Adolescentes y Redes Sociales en Internet (con la participación de: Belén Albornoz, Florencia Barindelli, Chantal Bernier, Miguel Cillero, José Clastornik, Rosario Duaso, Carlos G. Gregorio, Esther Mitjans, Federico Monteverde, Erick Iriarte, Thiago Tavares Nunes de Oliveira, Lina Ornelas, Leila Regina Paiva de Souza, Ricardo Pérez Manrique, Nelson Remolina, Farith Simon y María José Viega) realizado en Montevideo los días 27 y 28 de julio de 2009.

Esta edición estuvo a cargo del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) y del Instituto de Investigación para la Justicia (IIJusticia).
Se terminó de imprimir en julio de 2011 en México, D.F.

Esta edición consta de 1500 ejemplares

IIJusticia

ifai

IDRC CRDI

Canadian International Development Agency

Agence canadienne de développement international