# 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 ado-

[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.

lescentes 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.

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 asocia-

[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".

ciones 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.

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