APÉNDICE DOCUMENTAL

*Memorándum de Montevideo**

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes

I. *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, 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*

* Recomendaciones adoptadas en el *Seminario Derechos, Adolescentes y Redes Sociales en Internet* (con la participación de: Belén Albornoz, Florencia Barindeli, 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 28/7/2009.

Público Federal de Brasil e a Google[1] (1º/7/2008); la *Child Online Protection Initiative*[2] de la Unión Internacional de Telecomunicaciones (18/5/2009); la *Opinion 5/2009 on online social networking*,[3] del Grupo Europeo de Trabajo del art. 29 (12/6/2009); 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 16/7/2009).[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 su 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 sus 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, decidir los alcances de su vida privada, debe limitarse el poder tanto del Estado como de organizaciones privadas, de cometer

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_f.cfm/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* (17/10/2008); "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 art. 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.

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 e 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 documentos, directrices o recomendaciones a las niñas, niños y adolescentes, como sujetos especialmente protegidos y vulnerables respecto del tratamiento de sus datos personales. Asimismo deberán enfocar esfuerzos para promover o fortalecer una cultura de protección de datos en las niñas, niños y adolescentes.

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 responsa-

ble 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 el principio del interés superior[7] y el art. 16 de la CDN que determina:

> "*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 de 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 de 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.

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 aque-

[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).

[7] *Art. 3.1 de la CDN* — 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.

llos 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 las 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 actores involucrados y con ello responder a las particularidades locales y culturales.[8]

[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."

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.

4.3. 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 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, etcétera.

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]

[9] *ITU Guidelines for Policy Makers* #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".

[10] *Declaración de Principios sobre Libertad de Expresión,* de la Comisión Interamericana de Derechos Humanos de la OEA (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].

10. Se debe garantizar:

10.1. Que existan procesos judiciales y administrativos sencillos, ágiles, de fácil acceso y que sean 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 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.

[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.

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:

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 deben 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, etcétera.

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

[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".

[13] *ITU Guidelines for Policy Makers* #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".

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.

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 éstos 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 deberá tener en cuenta los mecanismos de controles parentales de acuerdo con la legislación de cada país, de los que deben darse una información clara.

[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."

[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".

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 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]

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*, 16/7/2009.

17 Ídem.

18 Ídem.

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]

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 da-

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, 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*, 16/7/2009.

tos personales de los usuarios con el consentimiento expreso de éstos. 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 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 técnicas y operativas 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.

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.

[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*, 16/7/2009.

[22] *ITU Guidelines for Policy Makers* #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".

7. *Consideraciones finales*

31. Las recomendaciones señaladas para los niños niñas, 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

*Memorando de Montevideu**

Memorando sobre a proteção de dados pessoais e da privacidade nas redes sociais da Internet principalmente en relação às crianças e adolescentes

1. *Considerações gerais*

A Sociedade da Informação e do Conhecimento, com ferramentas como a Internet e as redes sociais digitais, é uma oportunidade inestimável para o acesso e intercâmbio de informação, propagação de ideias, participação cidadã, diversão e integração social, especialmente através das redes sociais.

As crianças e adolescentes têm cada vez maior acesso aos diferentes sistemas de comunicação, permitindo-lhes obter todos os benefícios que estes sistemas oferecem. Entretanto, esta situação também levou a que o equilíbrio entre o exercício dos direitos fundamentais e os riscos ao usar estes sistemas chegasse ao seu limite—em termos de privacidade, honra, reputação, e intimidade, entre outros— da mesma forma como no caso de virem a ser vítimas de abusos —como por exemplo: discriminação, exploração sexual, pornografia— fazendo com que possa haver um impacto negativo para o seu desenvolvimento integral e vida adulta.

Na América Latina e o Caribe, bem como em outras regiões, estão sendo feitos esforços, dentro da diversidade social, cultural, política e normativa existente, para obter consenso e racionalidade visando estabelecer um equilíbrio entre a garantia dos direitos e a proteção diante dos riscos na Sociedade da Informação e do Conhecimento. Nesse sentido, podemos citar, entre outros, os mais recentes documentos: o Acordo que põe fim à disputa judicial entre o Ministério Público Federal do Bra-

* Recomendações adotadas no Seminário Direitos, Adolescentes e Redes Sociais na Internet (com a participação de Belén Albornoz, Carlos G. Gregorio, Chantal Bernier, Erick Iriarte, Esther Mitjans, Farith Simon, Federico Monteverde, Florencia Barindeli, José Clastornik, Leila Regina Paiva de Souza, Lina Ornelas, María José Viega Miguel Cillero, Nelson Remolina, Ricardo Pérez Manrique, Rosario Duaso e Thiago Tavares Nunes de Oliveira) realizado em Montevideu nos dias 27 e 28/7/2009.

sil e o Google[1] (de 1º/7/ 2008); o programa Proteção para Crianças online (CPO)[2] da União Internacional de Telecomunicações (de 18/5/2009); a Opinião 5/2009 sobre as redes sociais na Internet ,[3] do Grupo Europeu de Trabalho do Artigo 29° (de 12/7/2009); o Relatório de conclusões da investigação feita a partir de uma denúncia apresentada pela Clínica Canadense de Políticas Públicas para Internet e Interesse Público (CIPPIC. contra Facebook Inc.[4] (de 16/7/2009).[5]

As recomendações apresentadas a seguir são uma contribuição para que os diversos atores envolvidos da região se comprometam com essa questão, visando não só ampliar os aspectos positivos da Sociedade da Informação e do Conhecimento, incluindo a Internet e as redes sociais digitais, como também para prevenir aquelas práticas prejudiciais que serão muito difíceis de reverter, incluindo os impactos negativos das mesmas.

Qualquer abordagem sobre o tema requer a consideração de duas dimensões: Por um lado, o reconhecimento de que as crianças e adolescentes são titulares de todos os direitos, e portanto podem exercê-los em função de sua idade e maturidade, sendo suas opiniões consideradas em função da idade e maturidade. Por outro lado, considerar o fato de que por sua particular condição de desenvolvimento, elas têm o direito a uma proteção especial naquelas situações que possam ser prejudiciais para o seu desenvolvimento e os seus direitos. O direito à privacidade é um valor que toda sociedade democrática deve respeitar. Portanto, para garantir a autonomia dos indivíduos e decidir o âmbito da vida privada, o poder tanto do Estado como da organizações particulares deve ser limitado, visando impedir que cometam intromissões ilegais ou arbitrárias, na esfera pessoal. Em especial, a informação

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_f.cfm / http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm*

5 Outros documentos especialmente considerados: Resolução de Estrasburgo sobre Proteção da Privacidade nos Serviços de Redes Sociais (17/10/2008); "Recomendação sobre redes sociais" da Agência Espanhola de Proteção de Dados, "Estudo sobre a privacidade dos dados pessoais, privacidade e segurança da informação nas Redes Sociais online", realizado pelo Instituto Nacional de Tecnologias da Comunicação, INTECO e pela Agência Espanhola de Proteção de Dados (2009), "Declaração e Plano de Ação do Rio de Janeiro para Prevenir e Eliminar a Exploração Sexual de Crianças e Adolescentes" (novembro 2008), o Parecer 2/2009 sobre a proteção dos dados pessoais das crianças do Grupo Europeu de Trabalho do Artigo 29° (2009); o Relatório de Análises e Propostas em matéria de Acesso à Informação e Privacidade na América Latina do Monitor de Privacidade e Acesso à Informação, e os documentos de eLAC 2007 e 2010.

pessoal de crianças e adolescentes deve ser protegida, sem que a sua dignidade seja afetada, já que eles têm uma expectativa razoável de privacidade ao compartilhar sua informação em ambientes digitais, uma vez que consideram estarem em uma área privada.

Neste sentido, é importante recordar a importância de as crianças e adolescentes serem consultados e suas opiniões consideradas em todas as medidas que forem implementadas nesta área.

A sociedade civil espera dos agentes econômicos a declaração de adesão a princípios, atitudes e procedimentos que garantam os direitos das crianças e adolescentes na Sociedade da Informação e do Conhecimento.

Em termos da erradicação da pornografia infantil na Internet, espera-se um esforço conjunto de todos os atores responsáveis —governos, polícia, provedores de acesso e de conteúdo, sociedade civil, setor privado— nacional, regional e internacionalmente para mobilizar e envolver a um número cada vez maior de empresas, organizações públicas e sociedade civil.

Para estas recomendações, foram consideradas as particularidades de gênero e a diversidade cultural existente na América Latina, bem como um leque de políticas e de normativas sobre a forma de enfrentar o fenômeno da Sociedade da Informação e do Conhecimento, com especial ênfase na Internet e nas suas redes sociais.

Os organismos multilaterais deverão incluir, em seus documentos, diretrizes ou recomendações para as crianças e adolescentes, como sujeitos particularmente vulneráveis e que portanto devem ser especialmente protegidos com respeito ao tratamento de seus dados pessoais. Os organismos devem também concentrar esforços para promover ou fortalecer nas crianças e adolescentes uma cultura de proteção de dados.

Estas recomendações utilizam como referente normativo fundamental a Convenção das Nações Unidas sobre os Direitos da Criança (CDC), instrumento ratificado por todos os países da região, reconhecendo claramente a responsabilidade da sociedade e do Estado, compartilhada dentro dos seus respectivos âmbitos, visando a proteção da infância e da adolescência. As recomendações partem de três considerações fundamentais: o reconhecimento do relevante papel que a família ocupa, ou de quem for responsável pelo cuidado das crianças e adolescentes no processo de educação sobre o uso responsável e seguro de ferramentas como a Internet e as redes sociais digitais, bem como na proteção e garantia de seus direitos; a necessidade de que todas as medidas que forem tomadas priorizem o melhor interesse da criança e do adolescente; guardando um equilíbrio entre as necessidades de proteção contra a vulneração de seus direitos e o uso responsável dessas ferramentas que representam formas de exercício dos seus direitos; e, que todo aquele que de qualquer forma se beneficar através da

Internet e das redes sociais digitais seja responsável pelos serviços que fornecer e portanto deverá assumir a responsabilidade nas soluções para a problemática que for gerada.

2. *Recomendações para os Estados e instituições educativas para a prevenção e educação de crianças e adolescentes*

Toda ação em matéria de proteção dos dados pessoais e da vida privada das crianças e adolescentes[6] deve considerar o princípio do melhor interesse da criança[7] e o artigo 16 da CDC que determina que:

> *"(1).* Nenhuma criança será objeto de interferências arbitrárias ou ilegais em sua vida particular, sua família, seu domicílio, ou sua correspondência, nem de atentados ilegais a sua honra e a sua reputação". *(2).* A criança tem direito à proteção da lei contra essas interferência ou atentados".

É prioritária a prevenção, —sem negligenciar uma abordagem jurídico-regulamentar— para enfrentar os aspectos identificados como de risco na Sociedade da Informação e do Conhecimento, em especial na Internet e nas redes sociais, principalmente através da educação, considerando a participação ativa das próprias crianças e adolescentes, dos pais ou de quem estiver a cargo do seu cuidado e dos educadores, levando em consideração como princípio fundamental o melhor interesse das crianças e adolescentes.

Para isto, devem ser consideradas as seguintes recomendações:

1. Os Estados e as instituições educativas devem considerar o papel dos pais, ou de quem tiver sob sua responsabilidade o cuidado das crianças e adolescentes, na formação pessoal deles, o que inclui o uso responsável e seguro da Internet e das redes sociais digitais. É tarefa do Estado e das instituições educativas fornecer informação e reforçar as capacidades dos pais e das pessoas responsáveis, com relação aos eventuais riscos que as crianças e adolescentes enfrentam nos ambientes digitais.

2. Qualquer medida que envolva o controle dos meios de comunicação tem que respeitar o princípio de proporcionalidade, portanto deve ser determinado que a mesma vise a proteger e a garantir os direitos que estiverem de acordo ao objetivo perseguido, não existindo outra medida que permita obter os mesmos resultados e seja menos restritiva de direitos.

3. É importante transmitir claramente às crianças e adolescentes que a Internet não é um espaço sem regras, impune ou sem responsabilidades. Devem ser alertados para não se deixarem enganar com a aparente sensação de que ali vale tudo, porque todas as ações têm consequências. Devem ser educados no uso responsável e seguro da Internet e das redes sociais digitais. Destacando:

3.1. A participação anônima ou usar pseudônimos é possível nas redes sociais digitais. O processo educativo deve refletir sobre os aspectos positivos do uso de pseudônimos como meio de proteção. Um uso responsável —entre outras coisas— implica não utilizar desses recursos para enganar ou confundir as outras pessoas sobre a sua identidade real.

As crianças e adolescentes devem ser advertidos sobre a possibilidade de que quando pensam estar se comunicando ou compartilhando informação com uma pessoa determinada, em realidade pode se tratar de outra pessoa. Ao mesmo tempo é necessário advertir que a participação anônima ou com um pseudônimo permite a suplantação da identidade.

3.2. No processo educativo é necessário enfatizar o respeito à vida privada, à intimidade e à reputação de terceiras pessoas, entre outras questões. É importante que as crianças e adolescentes saibam que aquilo que elas divulguem pode vulnerabilizar os seus direitos e os de terceiros.

3.3. As crianças e adolescentes devem saber que a distribução de conteúdos proibidos pela lei local e regional (em especial a pornografia infantil), o assédio (em especial o assédio sexual), a discriminação, a promoção do ódio racial, a difamação, a violência, entre outros, são ilegais na Internet e nas redes sociais digitais, sendo puníveis por lei.

3.4. O processo educativo deve dar às crianças e adolescentes o conhecimento do uso responsável e seguro das políticas de privacidade, segurança e alertas com as que contam os instrumentos de acesso dos sites que as crianças e adolescentes são usuários frequentes, como por exemplo as redes sociais digitais.

3.5. É preciso promover uma política educacional —expressa em termos adequados à idade das crianças e adolescentes— que

[6] As expressões criança e adolescente são usadas com o sentido dado pela legislação nacional de cada país (conforme o país, a expressão criança poderá se referir a pessoas que não fizeram 12 ou 13 anos de idade, e adolescente a quem tiver mais de 12 ou 13 anos e menores de 18 anos. Nos países onde não foi introduzido juridicamente a categoria "adolescentes", passam a ser considerados os chamados "menores adultos" ou "menores púberes". No caso de Honduras, o menino para ser criança deve ser menor de 14 anos e a menina menor de 12 anos. Os adolescentes são maiores de 14 e as adolescentes maiores de 12 anos respectivamente e ambos menores de 18 anos).

[7] *Artigo 3.1 da CDC:* "Em todas as ações relativas às crianças, quer empreendidas por instituições de bem-estar social públicas ou privadas, tribunais, autoridades administrativas ou órgãos legislativos, o melhor interesse da criança será uma consideração principal".

inclua uma estratégia informativa e formativa, visando ajudá-los a gerenciar as potencialidades e os riscos derivados da Sociedade da Informação e do Conhecimento, em especial no uso da Internet e das redes sociais digitais.

3.6. Também é preciso informar sobre os mecanismos de proteção e sobre as responsabilidades civis, penais ou administrativas existentes quando os próprios direitos ou os de terceiros são vulnerados na rede.

3.7. Deve-se advertir do perigo que supõe o denominado roubo e/ou suplantação de identidade, passíveis de ocorrer nos ambientes digitais que induzem ao engano.

3.8. É necessário explicar para as crianças e adolescentes, com uma linguagem de fácil compreensão, o espírito das leis sobre proteção de dados pessoais e sobre proteção da vida privada, de tal modo que possam captar a ideia da importância do respeito à privacidade das informações pessoais de cada um deles e dos demais.

3.9. É necessário educar para a incerteza sobre a veracidade dos conteúdos e a validação das fontes de informação. É preciso ensinar crianças e adolescentes a pesquisar e a discriminar as fontes.

4. Recomenda-se enfaticamente a promoção de uma educação sólida e completa sobre a Sociedade da Informação e do Conhecimento, principalmente focada no uso responsável e seguro da Internet e das redes sociais digitais, por meio de:

4.1. A inclusão nos planos de estudos, em todos os níveis educativos, de informação básica sobre a importância da vida privada e da proteção dos dados pessoais, e demais aspectos indicados no numeral três.

4.2. A produção de matérial didático, principalmente audiovisuais, páginas web e ferramentas interativas (tais como jogos online. onde aparecem as potencialidades e os riscos. Estes materiais deverão incluir informação sobre os mecanismos de proteção dos direitos.

A natureza destas questões e materiais exige a participação e discussão dos mesmos por parte de todos os atores envolvidos e com isso responder às particularidades locais e culturais.[8]

[8] Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas. Items 3,4: 3.“ ... É muito importante que a produção de material seja local e que reflita a legislação do lugar, bem como os respectivos padrões culturais, fator essencial em qualquer campanha de segurança dentro da Internet e para qualquer material de capacitação”. *4.* “... Na produção de material educativo é importante levar em consideração que para quem não estiver familiarizado com a tecnologia não será fácil o seu uso. Portanto, é importante garantir que o material relativo à segurança esteja disponível tanto em material impresso como em outros formatos, pensados para fazer com que quem for usá-los possa se sentir mais cômodo, como por exemplo, as gravações em vídeo”.

4.3. Os educadores devem ser capacitados para facilitar a discussão e por em contexto as vantagens e os riscos da Sociedade da Informação e do Conhecimento, e em especial da Internet e das redes sociais digitais; podendo contar para isso com o apoio das autoridades de proteção dos dados pessoais ou de todas aquelas organizações que trabalhem com esta questão em vários países.

4.4. As autoridades educativas —com o apoio das autoridades de proteção de dados (onde existirem), do setor acadêmico, das organizações da sociedade civil, do setor privado e, se necessário, com a cooperação internacional— devem ajudar os educadores e apoiar o trabalho nas áreas descritas.

5. As autoridades competentes devem estabelecer mecanismos para que os centros educativos resolvam os conflitos gerados em consequência do uso da Internet e das redes sociais digitais por parte das crianças e adolescentes, com um sentido didático, sempre considerando o interesse superior dos mesmos, sem vulnerar direitos e garantias, em particular o direito à educação.

3. *Recomendações para os Estados sobre o marco legal*

O marco legal que regula a Sociedade da Informação e do Conhecimento na região —em particular a Internet e as redes sociais digitais— avança lentamente em comparação com o desenvolvimento de novas aplicações e conteúdos, tendo uma série de vácuos e gerando tensões importantes nos valores que lhe inspira e na forma de proteger os diferentes direitos. No entanto, existe algum nível de consenso, que considera haver suficientes princípios fundamentais e constitucionais para iluminar as decisiões que forem tomadas nesta matéria. É importante fazer a criação, reforma ou harmonização normativa consideradando primordialmente o melhor interesse da crianças e do adolescentes, considerando principalmente:

6. Que a proteção dos dados pessoais exige o desenvolvimento de uma normativa nacional, aplicável ao setor público e privado, contendo os direitos e princípios básicos, reconhecidos internacionalmente, bem como os mecanismos para a sua efetiva aplicação. Os Estados deverão considerar principalmente, na criação e no desenvolvimento destas regulamentações, as crianças e adolescentes.

7. A importância de se assegurar que qualquer ação ou omissão contra uma criança ou adolescente, que seja considerada ilegal no

mundo real, tenha o mesmo tratamento no mundo virtual, sempre garantindo o bem-estar e a proteção integral dos seus direitos.[9]

8. Os Estados devem legislar o direito que as crianças e os adolescentes têm, seja diretamente ou por meio de seus representantes legais, de solicitar o acesso à informação que for sobre elas mesmas e que estiver nas bases de dados tanto públicas como privadas, bem como a retificação ou o cancelamento de tal informação sempre que for necessário, assim como o direito a se opor ao uso destas informações para qualquer fim.

9. É importante desenvolver uma adequada regulação do funcionamento dos centros de acesso à Internet (públicos ou privados), podendo incluir, por exemplo, a obrigação de se utilizar mensagens de advertência, filtros de conteúdo, acessibilidade para as crianças e adolescentes, etc.

4. Recomendações para a aplicação das leis por parte dos Estados

Nos últimos anos, chegaram aos Tribunais de Justiça muitos conflitos ou violações de direitos como consequência da difusão de dados pessoais, invasão da vida privada, difamações pela Internet e pelas redes sociais digitais. Algumas decisões tem mostrado que o papel dos juízes para decidir situações novas está em conformidade com os princípios fundamentais. No entanto, a proporção de conflitos que têm um real acesso à justiça é mínima.

Os sistemas judiciais têm um papel muito importante para assegurar de um bom uso da Internet e das redes sociais digitais. As sanções civis e penais devem ser aplicadas não só para retificar os direitos vulnerados, mas também para dar aos cidadãos e às empresas regras claras sobre a interpretação das leis e dos princípios fundamentais.[10]

[9] Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas. Item 2: "Estabelecer, *mutatis mutandis*, que todo ato contra uma criança, que for ilícito no mundo real, também seja ilegal no mundo virtual, sendo válida para o mundo virtual a normativa relativa à proteção e privacidade dos dados pessoais de quem for considerado menor de idade".

[10] Declaração de Princípios sobre Liberdade de Expressão, da Comissão Interamericana de Direitos Humanos da OEA (Outubro de 2000): "*10.* As leis de privacidade não devem inibir ou restringir a investigação ou difusão de informações que sejam do interesse público. A proteção à reputação deve ser garantida por meio de sanções civis nos casos em que a pessoa ofendida for um funcionário ou indivíduo público ou estiver envolvida, de alguma forma, em um assunto de interesse público. Caso contrário, deve provar-se que o comunicador demonstrou negligência na sua conduta em obter as informações, fossem elas falsas ou verdadeiras, que tinha a intenção de causar danos à pessoa e conhecimento de que estava difundindo notícias falsas". [Aprovada durante o 108° Período Ordinário de Sessões da CIDH]

10. Deve-se garantir:

10.1. Que existam processos judiciais e administrativos simples, rápidos, de fácil acesso e que sejam tramitados com prioridade pelos tribunais e autoridades responsáveis.
É preciso fortalecer o uso da responsabilidade civil extracontratual objetiva como mecanismo regulatório para garantir os direitos fundamentais nas aplicações na Sociedade da Informação e do Conhecimento, na Internet e nas redes sociais digitais. As sanções judiciais pelos danos causados têm a vantagem de ser uma resposta imediata, eficiente e capaz de desencorajar os projetos perigosos. Este tipo de responsabilidade civil se fundamenta no melhor interesse da criança.[11]

10.2. As decisões tomadas nesta área deveriam ter a mais ampla difusão possível, utilizando técnicas de anonimização que garantam a proteção de dados pessoais.

10.3. Devia ser feita e difundida uma base de dados sobre casos e decisões (resoluções judiciais ou resoluções administrativas anonimizadas. vinculada à Sociedade da Informação e do Conhecimento, em especial a Internet e as redes sociais digitais. Esta base de dados seria um instrumento para que os juízes possam considerar o contexto nacional e internacional no qual estão decidindo.

11. É preciso estabelecer um canal de comunicação que permita às crianças e adolescentes apresentarem as denúncias que possam surgir devido à vulneração de seus direitos, em matéria de proteção de dados pessoais.

12. Promover o estabelecimento de organismos jurisdicionais especializados na área de proteção de dados.

13. Desenvolver capacidades nos atores jurídicos envolvidos em matéria de proteção de dados, com especial ênfase na proteção de crianças e adolescentes.

5. Recomendações em matéria de políticas públicas

Lembramos a necessidade de que o interesse superior da criança seja considerado como princípio reitor para qualquer ação nesta área, particularmente no desenvolvimento de políticas públicas inclinadas a regular as redes sociais digitais.[12]

[11] Neste sentido, destaca-se a intervenção dos Juizados Especiais do Brasil na proteção dos direitos dos cidadãos nas redes sociais na Internet.

[12] Opinião 5: 4. "A Opinião destaca a necessidade de considerar os Melhores Interesses da Criança, estabelecidos pela Convenção das Nações Unidas sobre os Direitos da Criança. O Grupo de Trabalho também quer destacar a importância deste princípio no contexto de Serviços de Redes Sociais ("SNS", na sigla em inglês)".

14. É recomendado considerar a implementação das seguintes políticas públicas:

14.1. Criação de mecanismos de resposta para o atendimento das vítimas de abusos na Sociedade da Informação e do Conhecimento, particularmente na Internet ou nas redes sociais digitais. Do mesmo modo, deve-se estabelecer sistemas de informação para que aquelas crianças e adolescentes que se sentirem preocupadas com os conteúdos na Internet ou nas redes sociais digitais possam rapidamente ser assessoradas e receber apoio.

Para isto, dever-se-iam criar medidas tais como a ajuda e denúncia online, números telefônicos gratuitos, centros de atendimento, etc.

14.2. Elaboração de protocolos para canalizar os conteúdos ilegais denunciados.[13]

15. Deveriam existir mecanismos regionais e internacionais para compartilhar a informação denunciada por particulares sobre estas ocorrências, em tempo real, para poder assim gerar políticas e mecanismos de proteção, de forma antecipada, devido a que os riscos gerados nas redes sociais digitais estão muito dispersos e não são plenamente advertidos.

16. Promover ações de sensibilização e divulgação de informação através da mídia e das próprias redes sociais, entre outros, porque são um veículo efetivo para promover um uso responsável e seguro das ferramentas da Sociedade da Informação e do Conhecimento.[14]

17. Promover o compromisso e a participação das associações públicas e privadas, assim como das redes nacionais de centros de acesso à Internet (onde houver), para garantir a participação na proteção

[13] Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas. Itens 5, 6 e 7: "5. Considerar a implementação de medidas adicionais destinadas a reduzir ou interromper o tráfego em módulos de acesso condicional ("CAM", na sigla em Inglês). *6.* Assegurar que seja estabelecido um mecanismo -e amplamente divulgadopara fornecer um meio de compreensão imediata, a fim de denunciar os conteúdos ilegais encontrados na Internet, como por exemplo uma linha de emergência nacional capaz de responder rapidamente e com a possibilidade de retirar ou deixar inacessível o material que for ilegal. *7.* Assegurar a existência de processos a nível nacional para garantir que qualquer CAM encontrado em um país seja canalizado para um recurso nacional e centralizado. Um exemplo é o National Center on Child Neglet (NCCAN)".

[14] Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas. Item 2: "É preciso considerar a ajuda da mídia para divulgar e promover as mensagens e campanhas de conscientização". Opinion 5: 3.4.

e nas campanhas de alerta sobre as potencialidades e os riscos da Internet e das redes sociais digitais.

18. Promover a geração de Conhecimento especializado com o fim de elaborar políticas públicas adequadas. Com relação aos comportamentos online de crianças e adolescentes, sugere-se investigar qual o papel que elas desempenham na recepção, produção, armazenamento e reprodução de conteúdos ilegais, bem como averiguar quais as medidas de proteção que elas mesmas desenvolvem, as motivações individuais e as coletivas de tais comportamentos, assim como os perigos reais aos que se enfrentam na Sociedade da Informação e do Conhecimento.

6. *Recomendações para a indústria*

As empresas provedoras de serviços de acesso à Internet, desenvolvedoras de aplicativos e de redes sociais digitais devem se comprometer decididamente a proteger os dados pessoais e da vida privada —em particular das crianças e adolescentes—, a cooperar com os sistemas de justiça nacionais, a desenvolver campanhas de prevenção e desenvolvimento de capacidades, entre outros instrumentos mediante compromissos ou códigos de conduta, que devem incluir:

19. Não permitir a recopilação, tratamento, difusão, publicação ou envio a terceiros de dados pessoais, sem o consentimento explícito da pessoa em questão. É necessário restringir o uso da informação recoletada para qualquer outra finalidade que não seja o motivo pelo qual a informação foi fornecida, principalmente na criação de perfis comportamentais. No caso das crianças, é fundamental considerar a proibição relativa ao tratamento de dados pessoais. No caso de adolescentes, é necessário considerar os mecanismos de controle parental de acordo com a legislação de cada país, devendo a informação ser dada de forma clara.[15]

20. Proteger a vida privada deveria ser a característica geral e por default em todas as redes sociais digitais, bases de dados e sistemas de comunicação, entre outros. As mudanças feitas no grau de privacidade do perfil de usuário devem ser simples e sem custo algum.

21. As regras sobre privacidade das páginas web, serviços, aplicativos, entre outros, deveriam ser explícitas, simples e claras, explicadas em uma linguagem adequada para crianças e adolescentes. Dever-se-á fornecer informação sobre os propósitos e finalidades para os quais os dados pessoais serão utilizados, assim como as transmissões de

[15] Os dados pessoais só podem ser publicados na Internet com o consentimento explícito do titular dos dados, ou se o próprio titular já os tiver tornado públicos.

dados para terceiros. Também devem indicar a pessoa ou pessoas responsáveis pelo tratamento da informação.

Também se deve oferecer um link para os "parâmetros de privacidade" no momento da inscrição, contendo uma explicação clara sobre a finalidade destes parâmetros.

Um aviso sobre o fato de que a rede social pré-selecionou os parâmetros também deve estar facilmente acessível, se for o caso, e um alerta de que podem sofrer mudanças a qualquer momento, de acordo com as preferências das crianças e dos adolescentes. Seria também desejável que sejam alterados os "parâmetros por default" dos conteúdos pessoais, para que só os amigos e as redes que o usuário determinar possam ter acesso a esses conteúdos.[16]

22. Toda rede social digital deve indicar explicitamente na parte relativa à "publicidade" contida em sua política de privacidade, sobre os anúncios publicitários e informar claramente, em especial às crianças e adolescentes, sobre o fato de que as informações pessoais dos perfis dos usuários são usadas para enviar publicidade segundo cada perfil. Deve-se evitar a publicidade que não for adequada para as crianças e adolescentes.[17]

23. Qualquer rede social digital deve indicar de maneira clara o motivo para exigir certos dados pessoais e particularmente, a data de nascimento no momento da inscrição e da criação de uma conta. Deve-se portanto explicar que a data de nascimento exigida tem como finalidade verificar a idade mínima permitida para se criar uma conta na rede social digital.

Também é preciso especificar como vão ser utilizados estes dados de caráter pessoal que precisam ser obrigatoriamente fornecidos.[18]

A indústria deverá implementar mecanismos para uma verificação fidedigna da idade de crianças e adolescentes para a criação de uma conta de usuário e/ou ter acesso a determinado conteúdo.

24. Toda rede social digital, sistema de comunicação ou base de dados deveria contar com formas de acesso à informação, rectificação e eliminação de dados pessoais, para usuários ou não-usuários, levando em consideração os fatores limitantes da lei.[19]

16 Diretiva de Privacidade do Canadá, Resumo do Caso "PIPEDA" (Lei de Proteção a Informações Pessoais e Documentos Eletrônicos) #2009-008, Relatório sobre a decisão judicial em relação à denúncia apresentada pela Clínica Canadense sobre Políticas de Internet e Interesse Público (CIPPIC, na sigla em inglês) contra Facebook Inc. Conforme a Lei de Proteção a Informações Pessoais e Documentos Eletrônicos, 16/7/2009.

17 Id.

18 Id.

19 O espírito deste último parágrafo é não excluir —pelo tempo que for preciso— a retenção dos dados dos usuários que possam ser necessários na investigação de delitos.

Toda rede social digital deve elaborar uma política acessível aos usuários em matéria de conservação da informação, em virtude da qual os dados pessoais dos usuários que desativaram sua conta sejam suprimidos totalmente dos servidores do serviço, após um período de tempo razoável. Além disso, é importante eliminar a informação de não-usuários, considerando um limite razoável de conservação quando tiverem sido convidados a ser parte das redes. As redes sociais digitais não devem utilizar a informação de não-usuários.

As duas opções que permitirem desativar e suprimir as contas devem ser totalmente visíveis para os usuários, que devem poder compreender o que cada opção significa para a gestão do serviço dos dados contidos em suas contas.[20]

É preciso informar aos usuários sobre as obrigações de privacidade com relação a terceiros. Esta política deve ser explícita, clara e visível.

25. Deve ser impedida a indexação dos usuários das redes sociais digitais por parte dos motores de pesquisa, a não ser que o usuário tenha optado por esta função. A indexação de informação de crianças deve estar proibida em todas as suas formas. No caso de adolescentes, estes devem autorizar de forma expressa a indexação de seus dados mínimos.

26. Toda rede social digital deve estabelecer as medidas necessárias para que quem desenvolva os diferentes aplicativos oferecidos pelo serviço (jogos, questionários, anúncios, entre outros) tenha limitado o seu acesso aos dados pessoais dos usuários, quando estes não forem necessários nem pertinentes para o funcionamento dos aplicativos.

A rede social tem que garantir que os terceiros que desenvolvem aplicativos em suas plataformas só possam ter acesso aos dados pessoais dos usuários com o consentimento expresso deles. A rede social digital deve garantir que os desenvolvedores de aplicativos solicitem apenas a informação indispensável, pertinente e não excessiva para o uso do aplicativo em questão.

Também é importante que sejam tomadas as medidas necessárias para impedir qualquer comunicação dos dados pessoais daqueles usuários que não tiverem eles próprios decidido expressamente instalar alguma aplicação.

20 Diretiva de Privacidade do Canadá, Resumo do Caso "PIPEDA" (Lei de Proteção a Informações Pessoais e Documentos Eletrônicos) #2009-008, Relatório sobre a decisão judicial em relação à denúncia apresentada pela Clínica Canadense sobre Políticas de Internet e Interesse Público (CIPPIC, na sigla em inglês) contra Facebook Inc. Conforme a Lei de Proteção a Informações Pessoais e Documentos Eletrônicos, 16/7/2009.

27. Estas recomendações se aplicam ao tratamento dos dados pessoais nas redes sociais digitais, mesmo que sua residência legal esteja fora da América Latina e o Caribe. Para facilitar o acesso dos usuários à justiça, cada provedor de redes sociais digitais deve fixar um domicílio ou representante legal nos países onde esta rede social tiver um uso significativo ou de acordo aos requerimentos do Estado.

As redes sociais digitais deverão estabelecer um serviço eficiente e eficaz de suporte aos usuários nestas questões. Este suporte deverá estar nas línguas oficiais utilizadas no país do usuário.

28. Os desenvolvedores de web sites, serviços, aplicativos e plataformas, entre outros, deverão estabelecer filtros de segurança, como meio complementar à educação, sensibilização e sanção.

29. A indústria deve estabelecer medidas de índole técnica e operativa para garantir a segurança da informação, em particular a integridade, disponibilidade e confidencialidade.

30. Para a erradicação da pornografia infantil na Internet, a indústria —em um esforço conjunto de todos os atores responsáveis– deve se comprometer no mínimo a:

30.1. Notificar às autoridades competentes todas as ocorrências de pornografia infantil detectadas em perfis de usuários de redes sociais digitais, para que seja possível abrir investigações e ações conforme o caso.

30.2. Preservar todos os dados necessários para a investigação por um prazo mínimo de seis meses ou entregar esses dados para as autoridades competentes, mediante autorização judicial.

30.3. Preservar os conteúdos publicados pelos usuários das redes sociais pelo mesmo prazo, e entregar esses conteúdos para as autoridades públicas, mediante autorização judicial.

30.4. Cumprir integralmente as legislações nacionais relativas a crimes cibernéticos praticados pelos cidadãos dos respectivos países da América Latina e o Caribe, ou feitos através da Internet desde as suas respectivas jurisdições nacionais.

30.5. Reformular o serviço de atendimento aos clientes e usuários para dar uma resposta em um tempo razoável a todas as reclamações formuladas por e-mail ou por correio pelas pessoas prejudicadas com a criação de comunidades falsas ou ofensivas.

30.6. Desenvolver uma tecnologia eficiente de filtragem e implementação de moderação humana, para impedir a publicação de fotografias e imagens de pornografia infantil no serviço das redes sociais digitais.

30.7. Desenvolver ferramentas por meio das quais as linhas telefônicas de ajuda a crianças e adolescentes possam encaminhar as denúncias para que os funcionários da empresa analisem, retirem os conteúdos ilegais e informem às autoridades competentes quando houver indícios de pornografia infantil, racismo ou outros crimes de ódio, bem como preservar todas as provas.

30.8. Retirar os conteúdos ilícitos, através de ordem judicial ou por requerimento de autoridade pública competente, preservando os dados necessários para a identificação dos autores desses conteúdos.

30.9. Desenvolver ferramentas de comunicação com as autoridades competentes, para facilitar a tramitação das denúncias, formulação de pedidos de remoção e/ou preservação de dados.

30.10. Informar adequadamente os usuários nacionais sobre os principais delitos cometidos nas redes sociais digitais (pornografia infantil, crimes de ódio, delitos contra a honra, entre outros).

30.11. Desenvolver campanhas de educação para o uso seguro e respeituoso das leis, da Internet e das redes sociais digitais.

30.12. Financiar a publicação de folhetos e a sua distribuição para crianças e adolescentes em escolas públicas, com informação para o uso seguro da Internet e das redes sociais.

30.13. É importante haver nos sites das redes sociais digitais os links de Sites Úteis, como por exemplo os de denúncia ou os telefones de ajuda para crianças e adolescentes.

7. *Considerações finais*

31. As recomendações indicadas para as crianças e adolescentes se extentem às outras pessoas (maiores de idade que devido à sua condição pessoal estiverem em uma posição de vulnerabilidade.

Grupos vulneráveis são todos aqueles relacionados aos dados sensíveis (conforme cada uma das legislações nacionais que geralmente incluem trabalhadores, dissidentes, pessoas com capacidades diferentes e suas famílias, imigrantes e emigrantes, entre outros.

32. Todos os atores envolvidos estão convidados a discutir e a interpretar estas recomendações. Do mesmo modo, é preciso buscar um diálogo constante sobre a questão abordada no presente documento. De maneira especial, apela-se ao cumprimento das obrigações dos Estados e à responsabilidade social empresarial para então encontrar as melhores formas de implementar este documento.

Montevideu, 28 de julho de 2009