



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

IIJusticia

Instituto de Investigación para la Justicia



Canadá

Investigación llevada a cabo con la ayuda de una subvención del Centro
Internacional de Investigaciones para el Desarrollo y de la Agencia
Canadiense de Desarrollo Internacional, Ottawa, Canadá







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 Acuerdo que pone fin a la disputa judicial entre el Ministerio Público Federal de Brasil y Google (de 1 de julio de 2008); la Child Online Protection Initiative del la Unión Internacional de Telecomunicaciones (del 18 de

mayo de 2009); la Opinion 5/2009 on online social networking, del Grupo Europeo de Trabajo del Artículo 29° (del 12 de Junio de 2009); el Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. (del 16 de Julio de 2009).

Las recomendaciones que se presentan a continuación son una contribución para que los diversos actores involucrados de la región se comprometan con el tema para extender los aspectos positivos de la Sociedad de la Información y Conocimiento, incluyendo Internet y las redes sociales digitales, así como prevenir aquellas prácticas perjudiciales que serán muy difíciles de revertir, así como los impactos negativos que las mismas conllevan.

Cualquier acercamiento al tema requiere que se consideren dos dimensiones. Por un lado el reconocimiento que niñas, niños y adolescentes son titulares de todos los derechos, y por tanto pueden ejercerlos en función de su edad y madurez, además que sus opiniones deben ser consideradas en función de sus edad y madurez, por otro, el hecho de que por su particular condición de desarrollo tienen el derecho a una protección especial en aquellas situaciones que pueden resultar perjudiciales para su desarrollo y derechos. 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 intromisiones ilegales o arbitrarias, en dicha esfera personal. En particular debe protegerse la información personal de niñas, niños y adolescen-

1. http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/?searchterm=google

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.





tes 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 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.

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 debe considerar el principio del interés superior 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.

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

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. Artículo 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”.





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 actores involucrados y con ello responder a las particularidades locales y culturales.

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.





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.

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 mis-

mos 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.

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. Se debe garantizar:

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.”

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.”





10.1. 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.

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.

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.

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.

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.

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 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.

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.

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 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.

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.

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

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.

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."





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.

22. Toda red social digital debe indicar explícitamente en la parte relativa a la “publicidad” contenida en su política de privacidad, sobre los anuncios publicitarios e informar claramente, en especial a niñas, niños y adolescentes, sobre el hecho de que las informaciones personales de los perfiles de los usuarios se emplean para enviar publicidad según cada perfil. Se deberá evitar publicidad que no sea adecuada para las niñas, niños y adolescentes.

23. Toda red social digital debe indicar de manera clara la razón que motiva el exigir ciertos datos personales y en particular, la fecha de nacimiento en el momento de la inscripción y la creación de una cuenta. Se debe por tanto explicar que la fecha de nacimiento exigida tiene por objeto el poder verificar la edad mínima permitida para poder crearse una cuenta en la red social digital. Se debe precisar igualmente cómo se van a utilizar estos datos de carácter personal que hay que facilitar de manera obligatoria. La industria deberá implementar mecanismos para una verificación fehaciente de la edad de niñas, niños y adolescentes para la creación de una cuenta de usuario y/o acceder a determinado contenido.

24. Toda red social digital, sistema de comunicación o base de datos debería contar con formas de acceso a la información, rectificación y eliminación de datos personales, para usuarios o no usuarios, tomando en consideración las limitantes de la ley. Toda red social digital debe elaborar una política accesible a los usuarios en materia de conservación de la información, en virtud de la cual los datos personales de los usuarios que han desactivado su cuenta sean suprimidos totalmente de los servidores del servicio, tras un periodo de tiempo razonable. Asimismo se deberá eliminar la información de no usuarios, considerando un límite razonable de conservación cuando han sido invitados a ser parte de las redes. Las redes sociales digitales no deben utilizar la información de no usuarios.

Las dos opciones que permitan desactivar y supri-

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.

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, July 16 2009.

17. Id.

18. Id.

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, July 16 2009.





mir las cuentas deben ser totalmente visibles para los usuarios, que deben poder comprender qué supone cada opción en cuanto a la gestión por parte del servicio de los datos contenidos en dichas cuentas. Se tiene que informar a los usuarios de las obligaciones de privacidad frente a terceros, dicha política debe ser explícita, clara y visible.

25. Debe impedirse la indexación de los usuarios de las redes sociales digitales por parte de los buscadores, salvo que el usuario haya optado por esta función. La indexación de información de niñas y niños debe estar prohibida en todas sus formas, en el caso de adolescentes éstos deben autorizar de forma expresa la indexación de sus datos mínimos.

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.

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.

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 elec-





trónico 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.

CONSIDERACIONES FINALES

31. Las recomendaciones señaladas para los niñas, niños y adolescentes se extiendan a otras personas (mayores de edad) que en razón de su condición personal se encuentre en una posición de vulnerabilidad. Se entienden por grupos vulnerables todos aquellos relacionados a los datos sensibles (según cada una de las legislaciones nacionales) que generalmente incluyen trabajadores, disidentes, personas con discapacidad y sus familias, inmigrantes y emigrantes, entre otros.

32. Se exhorta a todos los actores involucrados a discutir e interpretar las presentes recomendaciones. De igual modo se debe buscar un diálogo constante en esta materia a la luz del presente documento. De manera especial se apela al cumplimiento de las obligaciones de los Estados y a la responsabilidad social empresarial para encontrar las mejores formas de implementar el presente documento.

Montevideo, 28 de julio de 2009

Recomendaciones adoptadas en el Seminario Derechos, Adolescentes y Redes Sociales en Internet (con la participación de: Belén Albornoz, Florencia 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 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, July 16 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."





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

Memorando de Montevideo

IIJusticia

Instituto de Investigación para la Justicia



Canadá

Pesquisa realizada com apoio de uma subvenção do Centro Internacional
de Pesquisas para o Desenvolvimento (IDRC) y Agência Canadense para o
Desenvolvimento Internacional (CIDA/ACDI)







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 Brasil e o Google (de 1 de julho de 2008); o programa Proteção para Crianças online (CPO) da União Internacional de Telecomunicações (de 18 de maio

de 2009); a Opinião 5/2009 sobre as redes sociais na Internet, do Grupo Europeu de Trabalho do Artigo 29º (de 12 de Junho de 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. (de 16 de Julho de 2009).

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,

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 de outubro de 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 29º (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.





a informação 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 estar 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 beneficiar 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.

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 deve considerar o princípio do melhor interesse da criança 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 edu-

cativo 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 terceiros 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 distribuição 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.

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”.





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

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.

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 sé-





rie 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 decisões que forem tomadas nesta matéria. É importante fazer a criação, reforma ou harmonização normativa considerando 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.

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.

8. Orientações da União Internacional de Telecomunicações (ITU) para as decisões políticas. Itens 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."

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."

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.

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. 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 fundamen-





tais 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.

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.

10. Declaração de Princípios sobre Liberdade de Expressão, da Comissão Interamericana de Direitos Humanos da O.E.A. (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 108º Período Ordinário de Sessões da CIDH]

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

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.

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 sentem 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.

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.

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 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.

RECOMENDAÇÕES PARA A INDÚSTRIA

As empresas provedoras de serviços de acesso à Internet, desenvolvedoras de aplicativos e de redes

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).”

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 divulgado- para 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 Neglect (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.”. Opinião 5: 3.4.

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

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 recopilación, tratamento, difusión, publicación ou envío 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.

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 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.

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.

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.

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.

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.

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

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 de julho de 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.

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 de julho de 2009.





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.

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 respeitoso 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.

CONSIDERAÇÕES FINAIS

31. As recomendações indicadas para as crianças e adolescentes se estendem 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.

Montevideo, 28 de julho de 2009

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 Montevideo nos dias 27 e 28 de julho de 2009.





**Memorandum on the protection
of personal data and privacy in Internet social networks,
specifically in regard to children and adolescents**

Memorandum of Montevideo

IIJusticia

Instituto de Investigación para la Justicia



Canada

Research carried out with the aid of a grant from the International
Development Research Centre and the Canadian
International Development Agency, Ottawa, Canada





GENERAL CONSIDERATIONS

By providing tools such as the Internet and online social networks, the Information and Knowledge Society offers an invaluable opportunity to access and exchange information, as well as to spread ideas and to allow citizen participation, entertainment and social integration, particularly through social networks.

The growing access to a variety of communication systems by children and adolescents - with all the benefits that such access provides - has also lead to an extreme in what should be a balance between the exercise of basic rights on the one hand and safety on the other in matters of personal affairs, reputation, and privacy, among others. In these matters, through whose abuse children and adolescents can be victimized — such as discrimination, sexual exploitation, pornography and so on— could result in a negative effect on their overall development and on their adult lives.

Efforts are being made in Latin America and the Caribbean, as well as in other regions – and within the existing regulations and the social, cultural and political diversity – to attain a certain level of consensus and rationality and to establish a balance between the guarantee of rights and the protection from risks involved in the Information and Knowledge Society. On this topic, recently published documents are: Settlement of the judicial conflict between the Federal Public Ministry of Brazil and Google (dated July 1st,

2008); the Child Online Protection Initiative of the International Telecommunication Union (dated 18 May, 2009); Opinion 5/2009 on online social networking, by the Article 29 of the European Working Group (dated June 12th, 2009); the Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. (dated July 16th, 2009).

The following recommendations are a contribution to the commitment by the various involved parties to address the subject and advance the positive aspects of the Information and Knowledge Society, including the Internet and online social networks, as well as to prevent harmful practices that would prove extremely difficult to change, along with the negative effects they entail.

Any approach to the issue necessarily requires two dimensions: on one side, the acknowledgment that children and adolescents are fully entitled to their rights, and may therefore exercise them based on their age and maturity —and their opinions must also be considered based on their age and maturity— and on the other side the fact that, given their specific stage of development, they are entitled to special protection in situations that might prove harmful to their development and rights.

The right to privacy deserves the respect of every democratic society. Furthermore, to ensure the autonomy of individuals and to protect the scope of their privacy rights, the power of both the Sta-

1. Available at http://www.prsp.mpf.gov.br/sala-de-imprensa/noticias_prsp/noticia-7584/

2. Available at <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/index.html>

3. Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf

4. Available at http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm

5. Other particularly significant documents are: Strasbourg's Resolution on Privacy Protection in Social Network Services (October 17th, 2008); Recommendations regarding social networks by the Spanish Data Protection Agency, Study on privacy of personal data, privacy and information safety in online social networks by INTECO (Spanish acronym for National Institute of Communication Technology and the Spanish Data Protection Agency (2009), The Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents (November 2008), Advisory Opinion 2/2009 regarding protection of children's personal data by the Article 29 of the European Working Group (2009); the Report on Analysis and Proposals relative to Access to Information and Privacy in Latin America by the Privacy and Access to Information Monitor, and eLAC documents 2007 and 2010.





te and of private organizations must be limited in order to prevent illegal or arbitrary interference in their private lives. Specifically, protection is to be given to personal data of children and adolescents, without affecting their dignity as individuals, for they have a reasonable expectation of privacy when they share their information in digital environments and consider themselves to be in a private space.

In this respect, we must keep in mind the importance of consulting with children and adolescents, and for their opinions to be taken into account in whatever measures are implemented in these areas. Civil society expects that all parties in the economy adhere to the principles, attitudes and procedures oriented to securing the rights of children and adolescents in the Information and Knowledge Society.

With regard to the eradication of child pornography on the Internet, cooperation is expected from all responsible parties —governments, police, access and content providers, civil society, and the private sector— at the national, regional and international levels, so as to mobilize and involve a growing number of companies, public institutions and civil society organizations.

Prior to issuing these recommendations, the specific gender and cultural diversity features of Latin America and the Caribbean have been taken into account, as well as the variety of policies and regulations concerning approaches to the Information and Knowledge Society phenomena, focusing particularly on the Internet and online social networks.

Multi-lateral entities must include children and adolescents in their documents, guidelines and recommendations as specifically protected individuals who are vulnerable to the treatment given to their personal data.

The recommendations contained in this document refer to the United Nations Convention

on the Rights of the Child (henceforth referred to as CRC) as their main basis. The CRC has been ratified by all countries in the region and that clearly acknowledges the shared responsibility of the State and society, in their respective environments, in regard to the protection of children and adolescents. This is based on three basic aspects, which are: acknowledging the significant role played by families —or by whoever is responsible for the process of bringing up children and adolescents— in instructing them and protecting and ensuring their rights; the need for all measures adopted to prioritize the best interests of children and adolescents, while maintaining the balance between the need for protection against the violation of their rights and the responsible use of those tools representing ways of exercising their rights; and the fact that all those benefiting in any way from the Internet and online social networks are responsible for the services they provide and must therefore take responsibility for the solutions defined for the problems generated by these services.

RECOMMENDATIONS FOR STATES AND EDUCATION INSTITUTIONS FOR PREVENTION AND FOR EDUCATING CHILDREN AND ADOLESCENTS

All actions intended to protect the personal information and privacy of children and adolescents, must take into account the best interests principle, as well as Article 16 of the CRC, which reads as follows: “(1). No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, or correspondence, nor to unlawful attacks on his or her honor and reputation. (2). The child has the right to the protection of the law against such interference or attacks”.

Prevention is a priority —regardless of the poli-





cy, regulation or legal approach— in addressing through education the aspects identified as risks of the Information and Knowledge Society, specifically the Internet and digital social networks. This effort must include the active participation of children and adolescents themselves, as well as their elders and other individuals in charge of their care and teachers, and consideration of the best interests of children and adolescents as the basic principle.

For this purpose, the following recommendations are to be considered:

1. State and educational institutions must consider the role played by parents, or those responsible for the care of children and adolescents, in the education of the latter, including on the responsible and safe use of the Internet and online social networks. It is the duty of the State and educational institutions to provide information and to strengthen the capability of parents and responsible adults about the potential risk to which children and adolescents are exposed in digital environments.

2. All measures involving the control of communications must respect the proportionality principle, and it must be determined that they are intended to protect and guarantee rights in a manner appropriate to this objective, and that no other measures exist for attaining the same results that would be less restrictive of such rights.

3. Children and adolescents must be clearly informed that the Internet is in no way a space free of rules, punishment or responsibility. They should be warned against believing that

everything is allowed on the Internet, because each and every action will necessarily have consequences.

They should be instructed in the responsible and safe use of the Internet and online social networks, specifically in regard to:

3.1. Anonymous participation and the use of pseudonyms are both possible in online social networks. The process of education must reflect on the positive aspects of using pseudonyms as a means of protection, and the responsible use thereof, which includes not using them to deceive or confuse others regarding an actual identity, among other concerns.

Children and adolescents must be alerted to the possibility of their being in communication or sharing information with someone in fact different from the individual they think they are in communication with. They must also be cautioned about the possibility of phishing allowed by anonymous participation and the use of pseudonyms.

3.2. In the process of education it is necessary to emphasize, among other things, the respect for the personal affairs, privacy and reputation of others. It is important for children and adolescents to be aware that any data they reveal may end up endangering their rights and the rights of third parties.

3.3. Children and adolescents must be informed that distributing content banned by local and regional laws (particularly child pornography), harassment (particularly sexual harassment), discrimination, the promotion of racial hate,

6. The expression “children and adolescents” is to be used with the meaning set forth by the respective legislation in each country. Depending on the country, the term “children” may refer to individuals under the age of 12 or 13, and the term “adolescents” to individuals over that age and under 18 years old. In countries where the “adolescent” category has not been introduced in the applicable laws, the concept applies to the so-called “adult minors” or “pubescent minors”. In Honduras, for example, a boy is defined as an individual younger than 14, and a girl is an individual younger than 12 years of age, while adolescents are those over such ages but younger than 18.

7. Article 3.1 of CRC reads as follow: “In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration”.





defamation, and violence, among others are not legal on the Internet or in online social networks and are liable to legal punishment.

3.4. The learning process must provide knowledge regarding the responsible and safe use by children and adolescents of privacy and safety policies and alerts included in access instruments and websites frequently used by children and adolescents, such as online social networks.

3.5. Education policies —expressed in language consistent with the age of children and adolescents— must include an informational and developmental strategy to aid children and adolescents in managing the potential risks derived from the Information and Knowledge Society, specifically with regard to the use of the Internet and online social networks.

3.6. Information must be provided about protection mechanisms and the civil, criminal and administrative liability for the violation of one's own rights or the rights of others on the net.

3.7. Warnings must be made about the dangers of identity theft and impersonation that exist in online environments and that can lead to deceit.

3.8. It is necessary to explain to children and adolescents in an easily understood manner the spirit of legislation concerning the protection of personal data and privacy so that they may grasp the importance of respect for the privacy of the personal information of each individual, themselves included.

3.9. Education is necessary in regard to the uncertainty of the veracity of content and the validation of data sources. Children and adolescents

must be trained and taught how to search for and be discerning about sources.

4. It is particularly recommended that a comprehensive and continuing education about the Information and Knowledge Society be developed, especially on the responsible and safe use of the Internet and online social networks and in particular by means of:

4.1. Including, in all syllabuses at all educational levels, basic information on the significance of privacy and the protection of personal data and other aspects as mentioned in item three.

4.2. Producing educational material, specifically, audio-visual material, web pages and interactive tools (such as online games) showing both the potential and risk involved. Such material must include information related to the mechanisms for the protection of rights.

The nature of these topics and materials calls for the participation of and discussion by all parties involved in order to take into consideration local and cultural peculiarities.

4.3. Teachers must be trained in how to enable the discussion and place the advantages and risks of social networks of the Information and Knowledge Society in due context, with the possible support of authorities responsible for the protection of personal data and any and all entities that work on that subject in different countries.

4.4. The education authorities —supported by authorities responsible for the protection of data (if any), the academic sector, civil society organizations, private sector entities, and (when necessary) with the aid

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"; " ... 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".

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".





of international cooperation— must assist educators and support all work in the areas mentioned.

5. The appropriate authorities should establish guidelines by which schools and other educational programs can resolve incidents that arise in the usage of the Internet and online social networks by children and adolescents, using these incidents as an opportunity to educate but always bearing in mind the best interests of the children involved and without violating their rights or entitlements, in particular their right to education.

RECOMMENDATIONS FOR STATES REGARDING LEGAL FRAMEWORKS

The regional legal frameworks that regulate the Information and Knowledge Society—in particular the Internet and online social networks— have developed more slowly than the development of new applications and content, and have a series of gaps and significant tensions between the values that motivate them as well as inconsistencies in how they approach the protection of rights. Nevertheless, there is a degree of consensus acknowledging that there are sufficient fundamental and constitutional principles to support any decisions made in these matters.

The creation, amendment or coordination of regulations must consider, in the first place, the best interests of children and adolescents and should specifically take into account the following:

6. Protecting personal data involves the development of national regulations, applicable to the public and private sectors; such regulations ought to be in compliance with internationally acknowledged basic rights and principles as well as the mechanisms necessary for their effective enforcement. In creating and developing these regulations, States must especially consider children and adolescents.

7. Any action or inaction regarding a child or adolescent that is considered illegal in the real world must also be considered illegal in the virtual world, to always guarantee their well-being and the overall protection of their rights

8. States must legislate the right of children and adolescents—either directly or through their legal representatives—to request access to any information on them included in public and private databases, and to the rectification and removal of such information when necessary, in addition to their entitlement to express their opposition to the use of such information for any purpose whatsoever.

9. Proper regulations must be developed for the operation of locations (both public and private) that provide access to the Internet and this might include, for example, the obligation to use alert messages or content filters, support accessibility for children and adolescents, and so on.

RECOMMENDATIONS FOR STATES IN THE ENFORCEMENT OF LEGISLATION

In recent years, many conflicts and violations of rights resulting from the publication of personal data, the interference in private affairs and defamation on the Internet and online social networks have ended in court. Certain rulings have shown the role of judges in applying fundamental principles to new situations. However, the proportion of conflicts that reach the judicial system is minimal.

Judicial systems play a significant role in ensuring the proper use of the Internet and online social networks. Civil and criminal penalties must be applied not only to redress the violation of rights but also to clearly indicate to the public and to companies how laws and fundamental principles will be interpreted.



10. The following is to be guaranteed:

10.1. The existence of simple, speedy and easily accessible judicial and administrative processes, to be treated as a priority by the courts and the relevant authorities.

The use of objective non-contractual liability is to be strengthened as a form of regulatory mechanism for guaranteeing fundamental rights in the applications of the Information and Knowledge Society, Internet and online social networks. Judicial penalties that can be applied to the derived damages have the advantage of being a quick, efficient response capable of dissuading dangerous designs. This type of civil liability is founded on the child's best interests.

10.2. The settlements arrived at by these means, should be made public and widespread as possible with the use of anonymity techniques to guarantee the protection of personal data.

10.3. Development and publication of a database of cases and legal decisions (anonymized administrative resolutions or court orders) related to the Information and Knowledge Society, and in particular to the Internet and online social networks. This could yield a tool for judges to analyze the national and international context in which they are operating and making decisions.

11. The establishment of a communications channel for allowing children and adolescents to report violations of their rights with regard to the protection of personal data.

12. Promotion of the establishment of jurisdictional entities that specialize in data protection.

13. Development of the capabilities of legal parties involved in data protection, focusing on the protection of children and adolescents.

10. In this sense, the participation of the Special Courts of Brazil in the protection of citizens' rights in Internet's social networks is to be mentioned.

RECOMMENDATIONS REGARDING PUBLIC POLICIES

The need for the best interests of children to be the guiding principle for all measures adopted on this issue is to be borne in mind, specifically in the development of public policies intended to regulate online social networks.

14. The implementation of the following public policies is recommended:

14.1 Definition of response mechanisms for assisting the victims of abuse in the Information and Knowledge Society, particularly on the Internet or in online social networks. Likewise, information systems are to be created for providing assistance and quick support to children and adolescents concerned in any way about content on the Internet or in online social networks. For this purpose, it is possible to create mechanisms to aid online reporting, through toll free numbers, service centers, and so on.

14.2. Definition of protocols to channel the illegal content that is reported.

15. Creation of regional and international mechanisms for sharing information reported by private parties regarding these occurrences, in real time, in order to promptly generate protective policies and mechanisms. This is due to the type of problems involved in online social networks, which are often dispersed and not fully detected.

16. Promotion of efforts to raise public awareness and to spread information through the press, the mass media, as well as through the social networks themselves, among others, all of which are effective means for promoting the responsible and safe use of tools of the Information and Knowledge Society.



17. Promote the commitment and participation of public and private associations, as well as national networks of centers for accessing the Internet (if any), to ensure their participation in protection and in alert campaigns on the possibilities and risks involved in the Internet and online social networks.

18. To promote specialized research in order to develop appropriate public policy. With regard to the online behavior of children and adolescents, it is particularly recommended that research be conducted into the roles they play in the acquisition, production, storage and reproduction of illegal content, the protection measures they develop, the individual and collective motivations for such behaviors, as well as the actual dangers they face in the Information and Knowledge Society.

RECOMMENDATIONS FOR THE INDUSTRY

Companies in the business of providing access to the Internet and development of applications or online social networks must purposefully undertake the protection of private data and privacy – especially of children and adolescents – and cooperate with national judicial systems. This is in addition to implementing campaigns for prevention and development of capabilities, among other possible instruments, through formal commitments or codes of conduct that should include:

11. 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”.

12. 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 channeled towards a centralized, national resource. One example is the National Child Abuse Material Management Centre”.

19. A ban on the collection, processing, publication or sharing with third parties of personal data without the express prior consent of the individual whose data is involved. The use of information obtained is to be restricted only for the purpose for which it was originally obtained, particularly with regard to the creation of behavioral profiles. In the case of children, a ban on the handling of personal data is to be especially considered. Regarding adolescents, parent control mechanisms consistent with each country’s legislation —about which clear information is to be made available— should be taken into account.

20. The protection of privacy as a primary feature in all online social networks, databases and communication systems, among others. Making changes in the degree of privacy of user profiles must be simple and free of charge.

21. Explicit, simple and clear rules on the privacy of web pages, services, and applications, among others, explained in a language appropriate for children and adolescents.

Information is to be provided regarding the objectives and purposes for which personal data is to be used, as well as any communication thereof to third parties. Likewise, the name(s) of the individual(s) responsible for handling such information is (are) to be provided.

Also, a link to any “privacy options” is to be provided at the time of registration, with a clear explanation of the purpose of these options.

A notice should also be provided that the so-





cial network has pre-selected options, if applicable, and that they can be changed at any time according to the preferences of the children and adolescents.

It would also be desirable for the “default options” to be set such that personal content is accessible only to friends and any networks defined by the user.

22. All online social networks must expressly include (in the section concerning “advertising” contained in their privacy policies) indications about ads and clearly inform children and adolescents about whether personal data from user profiles is used to target advertising in accordance with every profile. Any improper advertising for children and adolescents is to be avoided.

23. Every online social network must clearly indicate the reason for requiring certain personal data, specifically dates of birth at the time of registration and account creation. It must be explained that the date of birth is required to verify the minimum age required for creating an account in the online social network.

The way in which this personal data (to be facilitated compulsorily) will be used is to be specified. The industry must implement mechanisms for the reliable verification of the age of children and adolescents upon the creation of user accounts and/or access to specific content.

24. All online social networks, communication systems and databases must include means to access, rectify and remove personal data for users and non-users, with consideration of applicable legal restrictions.

Every online social network must have a defined policy, accessible to users, with regard to the preservation of information according

13. 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”.

14. 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.

to which the personal data of users who have deactivated their accounts is fully removed from the service’s servers after a reasonable period of time. Likewise, all information on non-users is to be removed within a reasonable period after invitations have been forwarded to them to be part of the network. Online social networks should not use data regarding non-users.

The means to deactivate or remove accounts must be fully visible to users, who in turn must understand what is implied in each of the options with regard to how the service will handle the data contained in such accounts.

Users must be informed of the obligations relative to privacy with regard to third parties, and such policy is to be explicit, clear and visible.

25. The indexing of users of online social networks done by search engines is to be prevented, except in cases where the user has allowed such access. Indexing of data on children is to be banned in every form. In the case of adolescents, they must expressly authorize the indexing of their basic personal details.

26. All online social networks must establish the necessary means to restrict the access by third parties who develop the various applications offered by the service (games, questionnaires, notices, among others) to the personal data of users not necessary or relevant to the functioning of such applications.

Every social network must ensure that third parties who develop applications in their platforms may only access personal data of users with their express consent. Online social networks must ensure that third parties developers request nothing other than the data necessary and relevant to the use of their applications.

The adoption of measures necessary to avoid any





transfer of personal data of users who have not expressly chosen to install such applications is equally important.

27. These recommendations apply to the handling of personal data in online social networks, despite their legal domicile being outside Latin America and the Caribbean. In order to facilitate users' access to legal recourse, all companies providing online social networks must establish a domicile or legal representative in countries where such social networks have significant use or upon the request of government authorities. Online social networks must provide users with an efficient and effective support service with regard to the issues mentioned above. Such support must be provided in the official language(s) of the user's country.

28. Developers of web pages, services, applications, and platforms, among others, must define security filters as a supplementary means for the education, awareness and penalty instances.

29. The industry must establish technical and operational measures to guarantee data security, specifically: the integrity, availability and confidentiality of information.

30. In order to eradicate child pornography on the Internet, the industry must, as part of a joint effort of all responsible parties, commit to a minimum of:

30.1. Notifying the corresponding authorities of any occurrences of child pornography detected in the profiles of users of online social networks, in order to enable the necessary investigations and actions.

30.2. Preserving all data necessary for investigations for a minimum of six months or otherwise

surrender such data to the corresponding officials, upon court authorizations.

30.3. Preserving the content published by users of social networks for an equal period of time, and surrender such content to the appropriate officials, upon court authorization.

30.4. Fully complying with national laws regarding cybercrimes committed by citizens of the countries of Latin America and the Caribbean, or through Internet connections from these national jurisdictions.

30.5. Changing customer service so that it can respond within a reasonable period of time to all claims made by email or conventional mail by individuals who have been victimized by false or offensive communities.

30.6. Developing efficient filtering technology and implementing the involvement of human site administrators in order to prevent the publication of child pornography photographs and images in online social network services.

30.7. Developing tools to enable hotlines to which children and adolescents can direct reports in order to allow the company's officers to analyze and remove any illegal content and inform the appropriate authorities about the inclusion in such contents of signs of child pornography, racism or other hate crimes, preserving all related evidence.

30.8. Removing illegal content, whether by court order or upon the request of the relevant official authorities, while preserving the data necessary for identifying the authors of such content.

15. 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, July 16 2009.

16. Id.

17. Id.

18. The spirit of the last paragraph is to not exclude—for the time necessary—the withholding of data on users that might result necessary in investigating crimes.





30.9. Developing tools for communications with the relevant authorities in order to facilitate the management of reports, and the implementation of requests for the removal and preservation of data.

30.10. Properly informing national users on the common crimes committed in online social networks (child pornography, hate crimes, and attacks upon reputation, among others).

30.11. Developing educational campaigns on the law abiding and safe use of the Internet and online social networks.

30.12. Financing the publication and distribution of flyers to children and adolescents in public schools containing information concerning the safe use of the Internet and social networks.

30.13. Maintaining links in the sites of online social networks to sites for reporting problems or hotlines for the aid of children and adolescents.

FINAL CONSIDERATIONS

Recommendations made in the context of children and adolescents should also be applied to other individuals (adults) who may be in vulnerable situations due to their particular personal conditions. Vulnerable groups are defined as those related to sensitive data (according to each national legislation) that usually include workers, dissidents, the disabled and their families, immigrants and emigrants, among others.

32. All parties involved are urged to discuss and consider these recommendations. Also, in light of what has been set forth in this document, a permanent dialogue is to be sought concerning the issues herein. A special call is made with regard to the obligations pertaining to the States and to corporate social responsibility in order to implement this document in the best manner possible.

Montevideo, 28 July, 2009.

Recommendations adopted at the Seminar on Rights, Adolescents, and Internet Social Networks (with the participation of 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 and María José Viega), held in Montevideo on July 27 and 28, 2009.

19. 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, July 16 2009.

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, July 16 2009.

21. 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".



**Mémorandum sur le droit à la protection
des renseignements personnels et la vie privée dans les
réseaux sociaux sur l'Internet,
en particulier ceux des enfants et des adolescents**

Mémorandum de Montevideo



IIJusticia

Instituto de Investigación para la Justicia



Canada

Recherche réalisé grâce à une subvention du Centre de recherches pour
le développement international et l'Agence canadienne
de développement international, Ottawa, Canada







CONSIDÉRATIONS GÉNÉRALES

La société de l'information et de la connaissance, avec des outils tels que l'Internet et les réseaux sociaux numériques, constitue une opportunité inestimable pour l'accès à l'information et l'échange d'information, la diffusion des idées, la participation citoyenne, l'amusement et l'intégration sociale, notamment à travers les réseaux sociaux.

Les enfants et les adolescents ont de plus en plus d'accès aux divers systèmes de communication qui leur permettent de tirer profit de tout ce qu'ils représentent ; mais cette situation a aussi poussé à l'extrême l'équilibre entre l'exercice des droits fondamentaux et les risques –pour la vie privée, l'honneur, la réputation et l'intimité, parmi d'autres– qui, de même que les abus qu'ils peuvent souffrir –discrimination, exploitation sexuelle, pornographie, etc.–, peuvent avoir un impact négatif sur leur développement intégral et leur vie adulte. En Amérique Latine et aux Caraïbes, ainsi que dans d'autres régions, des efforts sont faits au sein de la diversité sociale, culturelle, politique et réglementaire existante en vue d'atteindre un consensus et une rationalité de sorte de créer un équilibre entre la garantie des droits et la protection face aux risques dans la société de l'information et de la connaissance. Dans ce sens, il est possible de citer certains des documents les plus récents : L'Accord qui met fin à la dispute judiciaire entre le Ministère Public Fédérale du Brésil et Google (du 1er juillet 2009); l'Initiative de protection des enfants en ligne de l'Union Internationale de Télécommunications (du 18 mai 2009); l'Opinion 5/2009 sur les réseaux sociaux en ligne, du Groupe Européen de Travail de l'Article 29 (du 12 juin 2009); le 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 Face-

book Inc. (du 16 juillet 2009).

Les recommandations présentées ci-dessous constituent une contribution pour que les divers acteurs de la région y impliqués s'engagent dans ce sujet pour élargir les aspects positifs de la Société de l'information et de la connaissance, y compris l'Internet et les réseaux sociaux numériques, ainsi que pour prévenir les pratiques préjudiciables qui seront très difficiles à modifier, de même que les impacts négatifs qu'elles provoquent.

Toute approche à ce sujet doit considérer deux dimensions. D'une part, la reconnaissance du fait que les enfants et les adolescents sont titulaires de tous les droits et, donc, ils peuvent les exercer en fonction de leur âge et leur maturité, en plus du fait que leurs opinions doivent être prises en considération en fonction aussi de leur âge et leur maturité ; d'autre part, le fait qu'en raison de leur condition particulière de développement, ils ont droit à une protection spéciale dans certaines situations qui peuvent s'avérer négatives pour leur développement et leurs droits.

Le droit à la vie privée est une valeur que toute société démocratique doit respecter. En conséquence, afin d'assurer l'autonomie des individus, de décider la portée de leur vie privée, il faut limiter tant le pouvoir de l'État que celui des organisations privées pour restreindre les intrusions illégales ou arbitraires dans cette sphère personnelle. En particulier, il faut protéger les informations personnelles des enfants et des adolescents sans affecter leur dignité en tant que personnes, car ils ont une expectative de confidentialité raisonnable lorsqu'ils partagent leur information dans des environnements numériques, vu qu'ils considèrent qu'ils se trouvent dans un espace privé.

Dans ce sens, il faut rappeler l'importance de consulter les enfants et les adolescents et de prendre leurs opinions en considération dans les mesures à appliquer dans ce sujet.

La société civile espère des agents économiques la déclaration d'adhésion aux principes, aux atti-

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





tudes et aux procédures qui garantissent les droits des enfants et des adolescents dans la Société de l'information et de la connaissance.

Quant à l'éradication de la pornographie infantile sur l'Internet, un effort conjoint de tous les acteurs responsables—des gouvernements, de la police, des fournisseurs d'accès et de contenu, de la société civile, du secteur privé— est souhaitable à l'échelle nationale, régionale et internationale pour mobiliser et impliquer un nombre de plus en plus grand d'entreprises, d'organisations publiques et de la société civile.

Les particularités de genre et la diversité culturelle en Amérique Latine et aux Caraïbes ont été prises en considération pour ces recommandations, ainsi que la diversité des politiques et des réglementations dans la manière de faire face au phénomène de la Société de l'information et de la connaissance, mettant notamment l'accent sur l'Internet et les réseaux sociaux.

Les organismes multilatéraux devront inclure les enfants et les adolescents en tant que sujets spécialement protégés et vulnérables par rapport au traitement de leurs données personnelles dans leurs documents, leurs directives ou leurs recommandations. De même, ils devront concentrer leurs efforts pour favoriser ou renforcer une culture de protection des données chez les enfants et les adolescents.

Ces recommandations se basent, notamment du point de vue réglementaire, sur la Convention des Nations Unies relative aux droits de l'enfant (CDE), un instrument ratifié par tous les pays de la région, où la responsabilité partagée par la société et par l'État, chacun dans son domaine respectif, dans la protection de l'enfance et l'adolescence, est clairement reconnue. Et ce, à partir de trois considérations fondamentales : la reconnaissance

du rôle pertinent qui joue la famille —ou les personnes chargées de la garde des enfants et des adolescents— dans le processus d'éducation sur l'utilisation responsable et sûre des outils comme l'Internet et les réseaux sociaux numériques et dans la protection et la garantie de leurs droits ; le besoin que toutes les mesures à prendre donnent la priorité à l'intérêt supérieur des enfants et des adolescents, tout en gardant un équilibre entre les besoins de protection contre la vulnération de leurs droits et l'utilisation responsable de ces outils qui représentent des formes d'exercice de leurs droits ; et que toute personne qui tire profit, quel qu'il soit, de l'Internet et des réseaux sociaux numériques est responsable des services fournis et, en conséquence, doit assumer sa responsabilité vis-à-vis des solutions aux problèmes que ceci entraîne.

RECOMMANDATIONS AUX ETATS ET AUX ETABLISSEMENTS EDUCATIFS POUR LA PREVENTION ET L'EDUCATION DES ENFANTS ET DES ADOLESCENTS

Toute action en matière de protection des renseignements personnels et de la vie privée des enfants et des adolescents doit considérer le principe de l'intérêt supérieur et l'article 16 de la CDE qui détermine que : «(1). Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. (2). L'enfant a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.»

La prévention —sans laisser de côté une approche de politiques, normative et judiciaire— est prioritaire pour faire face aux aspects de la Société de

5. D'autres documents spécialement considérés : Résolution sur la protection de la vie privée dans les services de réseaux sociaux (Strasbourg, le 17 octobre 2008) ; «Recommandation sur les réseaux sociaux» de l'Agence espagnole de protection des données, « Rapport sur la protection des données personnelles et la sécurité de l'information des réseaux sociaux en ligne », fait par l'Institut National des Technologies de la Communication, INTECO et par l'Agence Espagnole de Protection des Données (2009), la Déclaration et appel à l'action de Rio de Janeiro pour prévenir et éliminer l'exploitation sexuelle des enfants et des adolescents (novembre 2008), le Rapport 2/2009 sur la protection des renseignements personnels des enfants du Groupe de Travail Européen de l'Article 29 (2009) ; le Rapport d'Analyse et des Propositions en matière d'accès à l'information et la confidentialité en Amérique Latine du Moniteur de confidentialité et d'accès à l'information, et les documents d'eLAC 2007 et 2010.





l'information et de la connaissance, en particulier de l'Internet et des réseaux sociaux numériques, identifiés comme risqués, notamment à travers l'éducation, en considérant la participation active des enfants et des adolescents, leurs parents ou d'autres personnes à la charge de leur garde, et les éducateurs, prenant en considération comme principe fondamental l'intérêt supérieur des enfants et des adolescents.

Dans ce but il faut prendre en considération les recommandations suivantes:

1. Les États et les établissements éducatifs doivent tenir compte du rôle des parents ou des personnes responsables de la garde des enfants ou des adolescents dans leur formation personnelle, y compris l'utilisation responsable et sécuritaire de l'Internet et des réseaux sociaux numériques. L'État et les établissements éducatifs doivent fournir l'information et renforcer les capacités des parents et des personnes responsables sur les risques éventuels qui peuvent rencontrer les enfants et les adolescents dans les environnements numériques.

2. Toute mesure qui implique un contrôle des communications doit respecter le principe de proportionnalité ; en conséquence, il faut déterminer que son objectif est la protection et la garantie des droits, qu'elle est appropriée pour le but recherché et que c'est la seule qui permet d'obtenir ces résultats tout en étant la moins restrictive des droits.

3. Il faut transmettre clairement aux enfants et aux adolescents que l'Internet n'est pas un espace sans normes, impuni ou sans responsabilités. Il faut les avertir pour qu'ils ne soient pas trompés par l'apparente sensation que dans l'Internet tout est valable, car toutes les actions ont des conséquences. Il faut les éduquer dans l'utilisation responsable et

sécuritaire de l'Internet et des réseaux sociaux numériques. En particulier :

3.1. La participation anonyme ou l'utilisation de pseudonymes est possible dans les réseaux sociaux numériques. Le processus éducatif doit réfléchir sur les aspects positifs de l'utilisation de pseudonymes comme un moyen de protection et d'une utilisation responsable qui implique, parmi d'autres choses, de ne pas les utiliser pour tromper ou pour confondre les autres sur leur identité réelle.

Les enfants et les adolescents doivent être avertis sur la possibilité que, même s'ils croient être en communication ou partager des informations avec une personne déterminée, en réalité il peut s'agir d'une autre personne. En même temps, il faut leur avertir que la participation anonyme ou avec un pseudonyme rend possible le vol d'identité.

3.2. Pendant le processus éducatif il faut mettre l'accent sur le respect de la vie privée, de l'intimité et de la réputation des tierces personnes, parmi d'autres sujets. Il est important que les enfants et les adolescents sachent que ce qu'ils peuvent divulguer peut enfreindre leurs droits et ceux de tiers.

3.3. Les enfants et les adolescents doivent savoir que la distribution de contenus interdits par la réglementation locale ou régionales (notamment la pornographie infantile), l'harcèlement (notamment l'harcèlement sexuel), la discrimination, l'incitation à la haine raciale, la diffamation, la violence, etc. sont illégaux sur l'Internet et sur les réseaux sociaux numériques et ils sont punis par la loi.

3.4. Le processus éducatif doit apprendre aux enfants et aux adolescents l'utilisation responsable et sûre des politiques de confidentialité, de sécu-

6. Les expressions enfants et adolescents sont utilisées dans le sens que chaque pays leur donne dans la législation nationale. (Selon chaque pays, l'expression «enfants» pourra faire référence aux personnes de moins de 12 ou 13 ans, et «adolescent» aux personnes de plus de 13 ans mais de moins de 18 ans. Dans les pays où la catégorie «adolescents» n'a pas été incluse dans le cadre juridique, elle s'applique aux «mineurs pubères». Dans le cas de l'Honduras, «enfant garçon» est la personne de moins de 14 ans et «enfant fille» la personne de moins de 12 ans; «adolescents» sont les personnes de plus de ces âges et de moins de 18 ans).

7. Article 3.1 de la CDE «Dans toutes les décisions qui concernent les enfants, qu'elles soient le fait des institutions publiques ou privées de protection sociale, des tribunaux, des autorités administratives ou des organes législatifs, l'intérêt supérieur de l'enfant doit être une considération primordiale. »





rité et des alertes des instruments d'accès et des sites web qu'ils utilisent fréquemment tels que les réseaux sociaux numériques.

3.5. Il faut promouvoir une politique éducative – exprimée de façon compréhensible pour l'âge des enfants et des adolescents– qui comprenne une stratégie d'information et de formation pour les aider à gérer les potentialités et les risques causés par la Société de l'information et de la connaissance, notamment de l'utilisation de l'Internet et des réseaux sociaux numériques.

3.6. Il faut également les informer sur les mécanismes de protection et les responsabilités civiles, pénales ou administratives existantes lorsque leurs propres droits ou ceux des tiers sont enfreints dans le réseau.

3.7. Il faut leur avertir du danger qui suppose le vol et/ou la substitution d'identité qui peut se produire aux environnements numériques qui induisent en tromperie.

3.8. Il faut expliquer aux enfants et aux adolescents, en utilisant un langage facile à comprendre, l'esprit des lois sur la protection des données personnelles et la protection de la vie privée de sorte qu'ils puissent saisir l'idée de l'importance du respect de la confidentialité des informations personnelles d'eux-mêmes et des autres.

3.9. Il faut éduquer à propos de l'incertitude sur la véracité des contenus et la validation des sources d'information. Les enfants et les adolescents doivent apprendre à chercher et à discriminer les sources.

4. La promotion d'une éducation continue et complète sur la Société de l'information et de la connaissance est fermement recommandée, notamment pour l'utilisation responsable et sûre de l'Internet et des réseaux sociaux numériques, en particulier à travers:

4.1. L'inclusion dans les cursus, à tous les niveaux éducatifs, des informations de base sur l'importance de la vie privée et la protection des renseignements personnels, ainsi que des autres aspects indiqués au point 3.

4.2. La production de matériel didactique, notamment des audiovisuels, des pages web et des outils interactifs (tels que des jeux en ligne) où il y ait des potentialités et des risques. Ces matériels devront comprendre des informations sur les mécanismes de protection des droits

La nature de ces sujets et des ces matériels demande la participation et le débat de tous les acteurs concernés afin de répondre aux particularités locales et culturelles.

4.3. Les enseignants doivent être formés pour faciliter la discussion et placer dans son contexte les avantages et les risques de la société de l'information et de la connaissance, notamment de l'Internet et des réseaux sociaux numériques ; dans ce but, ils peuvent recevoir le soutien des autorités de protection des renseignements personnels ou de toutes les organisations qui travaillent dans ces sujets dans les différents pays.

4.4. Les autorités éducatives –avec l'appui des autorités de protection des données (là où elles existent), du secteur académique, des organisations de la société civile, du secteur privé et, si nécessaire, avec la coopération internationale– doivent aider les enseignants et appuyer le travail dans les domaines décrits.

5. Les autorités compétentes doivent créer des mécanismes pour que les établissements éducatifs puissent résoudre les conflits provoqués par l'utilisation de l'Internet et des réseaux sociaux numériques par les enfants et les adolescents, avec un sens didactique, en considérant toujours l'intérêt supérieur de ces enfants et adolescents, sans enfreindre aucun droit ou garantie, en particulier le droit à l'éducation.

RECOMMANDATIONS AUX ÉTATS SUR LE CADRE LÉGAL

Le cadre légal qui règle la Société de l'information et de la connaissance dans la région –en particulier l'Internet et les réseaux sociaux numériques– avance lentement par rapport au développement de nouvelles applications et contenus ; il a une série





de vides juridiques et de tensions importantes en ce qui concerne la façon de protéger les divers droits. Cependant, il existe un certain niveau de consensus sur le fait qu'il y a assez de principes fondamentaux et constitutionnels pour éclairer les décisions à prendre dans ce domaine.

La création, la réforme ou l'harmonisation réglementaire doivent se faire prenant comme considération essentielle l'intérêt supérieur des enfants et des adolescents, notamment il faut considérer que :

6. La protection des données personnelles demande le développement d'une réglementation nationale, applicable tant au secteur public qu'au secteur privé, qui contienne les droits et les principes fondamentaux reconnus internationalement et les mécanismes en vue de leur application effective. Pour la création et le développement de ces réglementations les États devront prendre spécialement en considération les enfants et les adolescents.

7. Il faut s'assurer que toute action ou omission contre un enfant ou un adolescent, considérée illégale dans le monde réel, reçoive le même traitement dans le monde virtuel, en garantissant toujours leur bien-être et la protection intégrale de leurs droits.

8. Les États doivent légiférer sur le droit des enfants et des adolescents, directement ou par l'intermédiaire de leurs représentants légaux, à demander l'accès à l'information sur eux-mêmes qui se trouve dans des bases des données tant publiques que privées, à rectifier ou à éliminer cette information si nécessaire, ainsi qu'à s'opposer à son utilisation à quelque fin que ce soit.

9. Il faut développer une réglementation adéquate pour le fonctionnement des centres d'accès à

Internet (publics et privés) qui peut comprendre, par exemple, l'obligation d'utiliser des messages d'avertissement, des filtres de contenu, l'accessibilité pour des enfants et des adolescents, etc.

RECOMMANDATIONS POUR L'APPLICATION DES LOIS PAR LES ÉTATS.

Pendant les dernières années il y a eu de nombreux conflits ou violations des droits comme conséquence de la diffusion de renseignements personnels, de l'invasion de la vie privée, des diffamations sur l'Internet et les réseaux sociaux numériques qui ont été portés devant les Tribunaux de Justice. Certaines décisions ont montré le rôle des juges pour prendre des décisions devant des situations nouvelles sur la base des principes fondamentaux. Cependant, la proportion de conflits qui ont un accès réel à la justice est minime.

Les systèmes judiciaires jouent un rôle très important pour assurer la bonne utilisation d'Internet et des réseaux sociaux numériques. Les sanctions civiles et pénales doivent être appliquées non seulement pour rectifier les droits enfreints mais aussi pour fournir aux citoyens et aux entreprises des règles claires sur l'interprétation des lois et des principes fondamentaux.

10. Il faut garantir:

10.1. L'existence de processus judiciaires et administratifs simples, agiles, d'accès facile, dont les démarches soient prioritaires pour les tribunaux et les autorités responsables.

Il faut renforcer l'utilisation de la responsabilité civile extracontractuelle objective comme mécanisme régulateur pour garantir les droits fondamentaux dans les applications dans la Société

8. Liste de contrôle #3 et #4 des Lignes directrices de l'ITU pour les Décideurs: « ... Il est très important, donc, que des matériels qui reflètent les lois et les normes culturelles locales soient produits à l'échelle locale. Ceci sera essentiel pour toute campagne de sécurité dans l'Internet ou tout matériel de formation qui soit développé. » ; 4. « ... Lorsque des matériels didactiques sont produits, il est important de prendre en compte que de nombreuses personnes qui viennent de connaître cette technologie ne se sentiront pas à l'aise en l'utilisant. Pour cette raison, il est important d'assurer que des matériels de sécurité soient mis à la disposition par écrit ou produits en utilisant d'autres moyens avec lesquels les nouveaux venus se sentiront plus à l'aise, par exemple, des vidéos. »





de l'information et de la connaissance, l'Internet et les réseaux sociaux numériques. Les sanctions judiciaires pour les dommages provoqués ont l'avantage d'être une réponse immédiate, efficace et capable de dissuader les conceptions dangereuses. Ce type de responsabilité civile est fondé sur l'intérêt supérieur de l'enfant.

10.2. Les décisions à prendre à ce sujet devraient être largement diffusées par l'intermédiaire de techniques d'anonymat qui garantissent la protection des renseignements personnels.

10.3. Il faudrait développer et diffuser une base de données sur des cas et des décisions prises (des jugements judiciaires ou des décisions administratives rendus anonymes) liée à la Société de l'information et de la connaissance, notamment à l'Internet et aux réseaux sociaux numériques; cette base de données serait un instrument pour que les juges puissent apprécier le contexte national et international où ils se trouvent.

11. Il faut créer un canal de communication qui permette aux enfants et aux adolescents de déposer les plaintes pouvant apparaître comme conséquence de la violation de leurs droits en matière de protection des renseignements personnels.

12. Il faut encourager la création d'organismes judiciaires spécialisés en matière de protection des données.

13. Il faut renforcer des capacités chez les acteurs juridiques impliqués en matière de protection des données, mettant notamment l'accent sur la protection des enfants et des adolescents.

RECOMMANDATIONS EN MATIÈRE DE POLITIQUES PUBLIQUES

Nous rappelons qu'il est nécessaire que l'intérêt supérieur de l'enfant soit considéré comme principe recteur de toute mesure à prendre à ce sujet, notamment en ce qui concerne le développement

9. Lignes directrices de l'ITU pour les Décideurs #2: «Établir, *mutatis mutandis*, que tout acte contre un enfant qui soit illégal dans le monde réel soit illégal en ligne, et que les règles de confidentialité et de protection des données pour des mineurs devant la loi soient aussi applicables.»

de politiques publiques visant à réglementer les réseaux sociaux numériques.

14. Il est recommandé de considérer l'application des politiques publiques suivantes:

14.1 La création de mécanismes de réponse pour assister les victimes d'abus dans la Société de l'information et de la connaissance, notamment dans l'Internet ou les réseaux sociaux numériques. Il faut créer également des systèmes d'information pour que les enfants et les adolescents qui aient un souci par rapport aux contenus dans l'Internet ou les réseaux sociaux numériques puissent avoir du conseil et du soutien rapidement.

Dans ce but, il est possible de créer des mesures telles que de l'aide et des plaintes en ligne, des numéros de téléphone gratuits, des centres d'assistance, etc.

14.2. La création de protocoles pour canaliser les contenus illégaux informés.

15. Il faudrait qu'il y ait des mécanismes régionaux et internationaux pour partager les informations dénoncées par des particuliers sur ces événements, en temps réel, afin de pouvoir générer des politiques et des mécanismes de protection de façon précoce, étant donné que les risques générés dans les réseaux sociaux numériques sont très dispersés et ils ne sont pas pleinement constatés.

16. Promouvoir des actions de sensibilisation et de diffusion des informations à travers les médias et les réseaux sociaux, parmi d'autres, car ceux-ci constituent un véhicule effectif pour encourager l'utilisation responsable et sûre des outils de la Société de l'information et de la connaissance.

17. Promouvoir l'engagement et la participation des associations publiques et privées, ainsi que des réseaux nationaux de centres d'accès à l'Internet (là où il y en a) afin d'assurer leur participation à





la protection et aux campagnes d'alerte sur les potentialités et les risques de l'Internet et des réseaux sociaux numériques.

18. Stimuler la génération de connaissances spécialisées dans le but d'élaborer des politiques publiques adéquates. Notamment, en ce qui concerne les comportements en ligne des enfants et des adolescents, il est conseillé de faire des recherches sur les rôles qu'ils jouent dans la réception, la production, le stockage et la reproduction des contenus illégaux, les mesures de protection qu'ils développent, les motivations individuelles et collectives de ces comportements, ainsi que les dangers réels qu'ils trouvent dans la Société de l'information et de la connaissance.

RECOMMANDATIONS POUR L'INDUSTRIE

Les entreprises qui fournissent les services d'accès à Internet, qui développent les applications ou les réseaux sociaux numériques, doivent s'engager fermement en matière de protection des renseignements personnels et de la vie privée –notamment des enfants et des adolescents–, s'engager à coopérer avec les systèmes de justice nationaux, à développer des campagnes de prévention et de renforcement des capacités, parmi d'autres instruments, à travers des engagements ou des codes de conduite qui doivent comprendre :

19. L'interdiction de collecter, traiter, diffuser, publier ou transmettre à des tiers des renseignements personnels sans le consentement explicite de la personne concernée. Il faut restreindre l'utilisation

10. Déclaration de Principes sur la Liberté d'Expression, de la Commission Interaméricaine des Droits de l'Homme de l'O.E.A. (Octobre 2000) : "10. Les lois sur la protection des renseignements personnels ne doivent ni empêcher ni limiter la recherche et la diffusion d'information d'intérêt public. La protection de la réputation doit être garantie seulement par le biais de sanctions civiles, dans les cas où la personne lésée est un fonctionnaire public ou une personne publique ou un particulier qui a volontairement joué un rôle dans des affaires d'intérêt public. En outre, dans de tels cas, il doit être établi que par la diffusion des avis, le communicateur avait l'intention d'infliger un dommage, qu'il était pleinement conscient de diffuser des informations fausses ou qu'il a fait preuve de négligence manifeste dans la recherche de la vérité ou de la fausseté de ces informations. » [Approuvée pendant la 108^e Période Ordinaire de Sessions de la CIDH]

11. Dans ce sens il faut signaler l'intervention des Tribunaux Spéciaux du Brésil dans la protection des droits des citoyens aux réseaux sociaux dans l'Internet.

de l'information recueillie dans un but différent de celui qui a motivé son traitement et, en particulier, de la création de profils de comportement.

Dans le cas des enfants il faudra considérer l'interdiction du traitement des renseignements personnels. Dans le cas des adolescents il faudra prendre en considération les mécanismes de contrôle des parents conformément à la législation de chaque pays, qui doivent être clairement communiqués.

20. La protection de la vie privée devrait être la caractéristique générale et, par défaut, dans tous les réseaux sociaux numériques, des bases de données et des systèmes de communication, etc. Les changements à effectuer dans le degré de confidentialité du profil de l'utilisateur doivent être simples et gratuits.

21. Les règles sur la confidentialité des pages web, des services, des applications, etc., devraient être explicites, simples et claires, exprimées dans un langage compréhensible pour les enfants et les adolescents.

Il faudra fournir des informations sur les buts et les fins de l'utilisation des renseignements personnels, ainsi que des transmissions effectuées à des tiers. Il faudra également indiquer les personnes responsables du traitement de l'information.

Il faut fournir aussi un lien vers les «paramètres de confidentialité» au moment de l'inscription, contenant une explication claire sur l'objet de ces paramètres.

Il faut rendre également accessible un avertissement sur le fait que le réseau social a présélectionné les paramètres, le cas échéant, et qu'ils peuvent être modifiés à tout moment selon les préférences des enfants et des adolescents.

Ce serait aussi souhaitable que les «paramètres par





défaut» des contenus personnels soient modifiés afin qu'ils ne soient accessibles qu'aux amis et aux réseaux que l'utilisateur détermine.

22. Tout réseau social numérique doit indiquer de façon explicite, dans la partie relative à la « publicité » contenue dans sa politique de confidentialité, les annonces publicitaires et informer de façon claire, notamment aux enfants et aux adolescents, que les renseignements personnels des profils des utilisateurs sont utilisés pour envoyer de la publicité selon chaque profil. Il faudra éviter la publicité non appropriée pour des enfants et des adolescents.

23. Tout réseau social numérique doit indiquer de façon claire la raison pour laquelle il exige certains renseignements personnels et, en particulier, la date de naissance au moment de l'inscription et de la création du compte. Il faut donc expliquer que la date de naissance demandée a pour objet de pouvoir vérifier l'âge minimum pour pouvoir créer un compte sur le réseau social numérique.

Il faut également préciser de quelle façon seront utilisés ces renseignements personnels qu'il faut fournir de façon obligatoire.

L'industrie devra mettre en pratique des mécanismes en vue de faire une vérification prouvée de l'âge des enfants et des adolescents pour la création d'un compte d'utilisateur et/ou pour accéder à un contenu déterminé.

24. Tout réseau social numérique, tout système de communication ou toute base de données devrait avoir des voies d'accès à l'information, de rectification et d'élimination des renseignements personnels pour des utilisateurs ou des non-utilisateurs,

12. Opinion 5: 4. «L'Opinion mettait l'accent sur la nécessité de prendre en considération le meilleur intérêt de l'enfant tel qu'il est également établi à la Convention des Nations Unies relative aux droits de l'enfant. Le Groupe de travail veut souligner l'importance de ce principe également dans le contexte des Services des Réseaux Sociaux.»

13. Lignes directrices de l'ITU pour les Décideurs #5, 6 et 7: «5. Considérer de prendre des mesures additionnelles pour interrompre ou réduire le trafic dans le CAM, par exemple, établir un service d'assistance téléphonique et développer des mesures qui bloquent l'accès à des sites web et des Forums de discussion d'Usenet connus pour contenir ou faire de la publicité de la disponibilité du CAM. 6. Assurer l'établissement d'un mécanisme et sa promotion largement afin de fournir un moyen de compréhension facile pour signaler le contenu illégal trouvé sur l'Internet, par exemple, un service d'assistance téléphonique qui ait la capacité de répondre rapidement et d'enlever ou de rendre inaccessible le matériel illégal. 7. Assurer l'existence de processus nationaux qui garantissent que tout CAM trouvé dans un pays soit canalisé vers une ressource centralisée, nationale. Un exemple est le Centre National de Gestion du Matériel d'Abus des Enfants.»

prenant en considération les limitations de la loi.

Tout réseau social numérique doit élaborer une politique accessible aux utilisateurs en matière de conservation des informations en vertu de laquelle les renseignements personnels des utilisateurs qui ont désactivé leur compte soient complètement éliminés des serveurs du service après une période de temps raisonnable. En outre, il faudra éliminer les renseignements des non-utilisateurs considérant une limite raisonnable de conservation quand ils ont été invités à faire partie des réseaux. Les réseaux sociaux numériques ne doivent pas utiliser les renseignements des non-utilisateurs.

Les deux options qui permettent aux utilisateurs de désactiver et de supprimer les comptes doivent être complètement visibles ; les utilisateurs doivent pouvoir comprendre ce que chaque option suppose quant à la gestion des données contenues dans ces comptes de la part du service.

Il faut informer les utilisateurs des obligations de confidentialité à l'égard des tiers ; cette politique doit être explicite, claire et visible.

25. Il faut empêcher l'indexage des utilisateurs des réseaux sociaux numériques par des navigateurs, sauf que l'utilisateur ait choisi cette fonction. L'indexage des renseignements des enfants doit être interdit sous toutes ses formes ; dans le cas des adolescents, ils doivent autoriser de façon expresse l'indexation de leurs renseignements minimums.

26. Tout réseau social numérique doit établir les mesures nécessaires pour limiter l'accès des tiers qui développent les diverses applications que le service offre (des jeux, des questionnaires, des annonces, etc.) aux renseignements personnels des





utilisateurs s'ils ne sont pas nécessaires ou pertinents pour le fonctionnement de ces applications. Le réseau social doit assurer que les tiers qui développent des applications dans leurs plateformes pourront accéder aux renseignements personnels des utilisateurs uniquement avec leur consentement exprès. Le réseau social numérique doit s'assurer que les tiers développeurs demandent uniquement les renseignements indispensables, pertinents et non excessifs pour l'utilisation de cette application. Il est important aussi de prendre les mesures nécessaires pour éviter toute communication de renseignements personnels des utilisateurs qui n'ont pas décidé de façon expresse par eux-mêmes d'installer une application.

27. Ces recommandations s'appliquent au traitement des renseignements personnels aux réseaux sociaux numériques, même si leurs adresses légales se trouvent en dehors de l'Amérique Latine et les Caraïbes. Pour faciliter l'accès des utilisateurs à la justice, chaque entreprise fournisseuse de réseaux sociaux numériques doit élire un domicile ou un représentant légal dans les pays où ce réseau social est utilisé de façon significative ou à réquisitoire de l'État. Les réseaux sociaux numériques devront créer un service efficace et efficient de support aux utilisateurs dans ces sujets dans les langues officielles utilisées dans le pays de l'utilisateur.

28. Les développeurs de pages web, de services, d'applications, de plateformes, etc., devront établir des filtres de sécurité comme un moyen complémentaire à l'éducation, la sensibilisation et la sanction.

29 L'industrie doit établir des mesures techniques et opérationnelles pour garantir la sécurité de l'information, en particulier l'intégrité, la disponibilité et la confidentialité.

30. Pour l'éradication de la pornographie infantile sur l'Internet, l'industrie —dans un effort conjoint de tous les acteurs responsables— doit s'engager au minimum à:

30.1. Notifier les autorités compétentes de toute apparition de pornographie infantile dans des profils des utilisateurs de réseaux sociaux numériques afin de pouvoir instruire les enquêtes et les actions correspondantes;

30.2. Préserver toutes les données nécessaires pour l'enquête pendant un délai minimum de six mois ou remettre ces données aux autorités compétentes, moyennant une autorisation judiciaire;

30.3. Préserver les contenus publiés par les utilisateurs des réseaux sociaux pendant le même délai et remettre ces contenus aux autorités publiques moyennant une autorisation judiciaire;

30.4. Appliquer de façon intégrale les législations nationales par rapport aux crimes cybernétiques commis par les citoyens des pays latino-américains et des Caraïbes ou moyennant des connexions à l'Internet faites depuis les juridictions nationales respectives;

30.5. Reformuler le service d'aide aux utilisateurs pour donner une réponse dans un délai raisonnable à toutes les réclamations, faites par courrier électronique ou par courrier postal, des personnes lé-

16. Liste de contrôle #2 des Lignes directrices de l'ITU pour les Décideurs : «Il faudrait également considérer d'assurer l'aide des médias dans la promotion de messages et de campagnes de sensibilisation.»

17. Opinion 5: 3.4. Les renseignements personnels sensibles ne pourront être publiés sur l'Internet qu'avec le consentement explicite de la personne concernée ou si la personne concernée a divulgué manifestement ces renseignements elle-même.

18. Id.

19. L'esprit de ce dernier paragraphe est de ne pas exclure —pour le temps nécessaire— la conservation des données des utilisateurs qui pourraient être nécessaires dans la recherche d'infractions.

20. Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt publique et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. En vertu de la Loi sur la protection des renseignements personnels et les documents électroniques, du 16 juillet 2009.





sées à cause de la création de communautés fausses au offensives;

30.6. Développer une technologie efficace de filtrage et de mise en pratique de modération humaine pour empêcher la publication de photographies et d'images de pornographie infantile sur le service des réseaux sociaux numériques;

30.7. Développer des outils à travers lesquels les lignes téléphoniques d'aide aux enfants et aux adolescents puissent acheminer les plaintes pour que les employés de l'entreprise analysent et retirent les contenus illégaux, qu'ils informent les autorités compétentes lorsqu'ils aient des indices de pornographie infantile, de racisme ou d'autres crimes de haine, et qu'ils préservent toutes les preuves;

30.8. Retirer les contenus illicites, soit moyennant une décision judiciaire, soit par mise en demeure d'une autorité publique compétente, tout en préservant les données nécessaires pour l'identification des auteurs de ces contenus;

30.9. Développer des outils de communication avec les autorités compétentes pour faciliter les démarches par rapport aux plaintes, la formulation des demandes de retrait et la préservation des données;

30.10. Notifier les utilisateurs nationaux de façon adéquate sur les principaux délits commis dans les réseaux sociaux numériques (pornographie infantile, crimes de haine, délits contre l'honneur, etc.);

30.11. Développer des campagnes d'éducation pour l'utilisation sûre et respectueuse des lois, de l'Internet et des réseaux sociaux numériques;

30.12. Financer la publication de brochures et leur distribution aux enfants et aux adolescents dans des

écoles publiques, contenant des informations pour l'utilisation sûre de l'Internet et des réseaux sociaux;

30.13. Maintenir un lien, dans les sites des réseaux sociaux numériques, avec des sites pour dénoncer ou des lignes d'aide aux enfants et aux adolescents.

CONSIDÉRATIONS FINALES

31. Les recommandations indiquées pour les enfants et les adolescents comprennent d'autres personnes (majeures) qui, en raison de leur condition personnelle, se trouvent dans une position de vulnérabilité.

Sont considérés des groupes vulnérables tous ceux en rapport aux données sensibles (selon chacune des législations nationales) qui comprennent généralement des travailleurs, des dissidents, des personnes handicapées et leurs familles, des immigrants et des émigrants, etc.

32. Tous les acteurs concernés sont priés de discuter et d'interpréter ces recommandations. Il faut également chercher un dialogue constant à ce sujet prenant en considération le présent document. De façon spéciale on fait appel à l'exécution des obligations des États et à la responsabilité sociale des entreprises pour trouver les meilleures formes de mettre en application le présent document.

A Montevideo, le 28 juillet 2009

Recommandations adoptées au Séminaire Droits, Adolescents et Réseaux Sociaux sur l'Internet (avec la participation 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 et María José Viega) tenu à Montevideo le 27 et le 28 juillet 2009.

21. Commissariat à la protection de la vie privée du Canada, Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2009-008, Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt publique et de politique d'Internet du Canada (CIPPIC) contre Facebook Inc. En vertu de la Loi sur la protection des renseignements personnels et les documents électroniques, du 16 juillet 2009.

22. Lignes directrices de l'ITU pour les Décideurs #13 : «Considérer le rôle qui peuvent jouer les outils techniques comme des programmes de filtrage et des logiciels pour la sécurité de l'enfant en appuyant et en complétant des initiatives d'éducation et de sensibilisation.»

