Colección Ensayos para la Transparencia de la Ciudad de México 2013

Invitamos a los lectores a consultar la página Web del Instituto, desde la cual tendrán acceso a todas nuestras publicaciones.

www.infodf.org.mx

La Morena No. 865 Local 1, Col. Narvarte Poniente,
Del. Benito Juárez, C.P. 03020, México, Distrito Federal
"Plaza de la Transparencia"
Tel. 5636-4636 (5636INFO) | www.infodf.org.mx | oip@infodf.org.mx

ensayos 24
PARA LA TRANSPARENCIA DE LA CIUDAD DE MÉXICO

La protección de datos personales de menores en la era digital.

Lina Gabriela Ornelas Núñez y
Samantha Alcalde Urbina

El Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF) pone a su disposición, la Colección de Ensayos para la Transparencia de la Ciudad de México, esfuerzo editorial dirigido a generar reflexión y análisis sobre el conocimiento y práctica de la transparencia, el acceso a la información, la protección de datos personales y la rendición de cuentas, en un contexto complejo como el Distrito Federal, una de las ciudades más grandes del mundo.

Comprometido con la promoción de la cultura de la transparencia, el instituto, a través de su línea editorial Ensayos Científicos, impulsa el desarrollo de investigaciones acerca de estos componentes esenciales para el fortalecimiento de las democracias modernas, convocando a reconocidos investigadores y académicos a debatir y aportar ideas y experiencias, a través de este género que consideramos apropiado a los propósitos de divulgación del InfoDF.

Los ensayos pretenden ser puntos de partida para impulsar debates, documentar tendencias recientes, e incorporar análisis críticos y novedosos. Su estructura libre, su tratamiento sintético, la variedad temática, convierten al ensayo en un recurso pedagógico para inducir a todo público en el conocimiento y reflexión, que sin duda son necesarios para construir un pensamiento analítico en torno a estos nuevos conceptos que acompañan el fortalecimiento de las democracias contemporáneas. Esperamos que los temas y el estilo personal de sus autores, inviten a la lectura y sobre todo, motiven su interés en participar en la discusión actual sobre estos temas y generar iniciativas que apoyen la consolidación de la cultura de trasnparencia en nuestra Ciudad de México.

24

LA PROTECCIÓN DE DATOS PERSONALES DE MENORES EN LA ERA DIGITAL

Lina Gabriela Órnelas Núñez
Samantha Alcalde Urbina

infodf

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Primera edición, Abril 2014
ISBN: 978-607-7702-04-7

ÍNDICE

LINA
ORNELAS NÚNEZ

Maestra en Cooperación Legal Internacional por la Universidad Libre de Bruselas.

Es experta en clasificación de información, transparencia, archivos, protección de datos y privacidad.

Se desempeñó durante 12 años en el sector público en México y Europa, de los cuales, nueve trabajó en el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) como Directora General de Clasificación y Datos Personales, y posteriormente como Directora General de Autorregulación en materia de protección de datos personales. Anteriormente trabajó para la Comisión Europea y las secretarías de Economía y Gobernación, en la que fungió como Directora General Adjunta en la Unidad para la Promoción y Defensa de los Derechos Humanos.

Ha coordinado subgrupos de trabajo de la Red Iberoamericana de Protección de Datos Personales; fue miembro del Consejo Editorial de la Revista de Protección de Datos de la Comunidad de Madrid Data Protection Review y actualmente de Future of Privacy Forum, junto con expertos en privacidad en Internet, así como miembro de la Asociación Internacional de Profesionales de Privacidad (IAPP). Ha publicado libros y numerosos artículos académicos entre los que destaca como coautora, junto con Alonso Gómez Robledo, del libro Protección de datos personales en México: el caso del Poder Ejecutivo; como coordinadora junto con Carlos Gregorio del libro Protección de datos personales de menores en las redes sociales digitales; coautora del capítulo sobre México en el libro Privacidad y derechos humanos 2005, 2006 y 2007 publicado por la organización Electronic Privacy Information Center (EPIC); y coordinadora, junto con José Luis Piñar Mañas, del libro La protección de datos en México, publicado por Tirant Lo Blanch y que aborda los aspectos relevantes de la Ley Federal de Protección de Datos en Posesión de Particulares y su Reglamento.

Fue Profesora Investigadora Asociada en el Centro de Investigación y Docencia Económicas, A.C. (CIDE), y actualmente es Jefa de Políticas Públicas y Relaciones con Gobierno para México, Centroamérica y El Caribe de Google.

SAMANTHA
ALCALDE URBINA

Licenciada en Derecho por la Universidad Iberoamericana, Campus Santa Fe, Ciudad de México. Por más de seis años ha trabajado en la Administración Pública Federal, en particular en Aeropuertos y Servicios Auxiliares.

Actualmente en el Instituto Federal de Acceso a la Información y Protección de Datos Personales se desempeña como Directora de Atención Regional.

En el Instituto Federal de Acceso a la Información y Protección de Datos ha participado en el grupo técnico de redacción de diversos instrumentos normativos, entre los que destacan la iniciativa de la Ley Federal de Protección de Datos Personales en posesión de los particulares y su reglamento, los Lineamientos del aviso de privacidad, y los Criterios generales para la instrumentación de medidas compensatorias sin la autorización expresa del IFAI. Ha participado de igual forma en la elaboración de diversas herramientas tutoriales sobre protección de datos personales.

Ha sido ponente en diversos foros nacionales y ha publicado diversos artículos, entre los cuales destacan: "Retos de la protección de datos personales en el sector público", *Seguridad de la información como una pieza clave en el rompecabezas de la protección de datos personales*, IFAI; y "Las redes sociales y la protección de datos personales en menores: perspectiva y retos", revista *Documentación*, núm. 20, Fundación Ciencias de la Documentación.

INTRODUCCIÓN

La humanidad debe al niño, lo mejor que puede darle[1]

Ya se ha vuelto un lugar común escuchar la denominación nativos digitales para referirse a las niñas, niños y adolescentes que hacen uso de la tecnología para comunicarse e interactuar. Dicho término fue utilizado por vez primera por Marc Prensky en el año 2001, quien de manera provocadora planteó la distinción entre nativos e inmigrantes digitales: los primeros son las personas para las cuales la tecnología digital ha sido su entorno de socialización, y los segundos son aquellos que se han tenido que adaptar a un nuevo lenguaje pero que piensan y procesan la información en forma fundamentalmente diferente a los "nativos".[2]

[1] Preámbulo de la Declaración de los Derechos del Niño de 1959 (ONU).

[2] De esta categorización se desprende una distancia entre generaciones de carácter cognitivo que según Prensky obliga a repensar parte de los contenidos educativos y principalmente la metodología educativa. "Different kinds of experiences lead to different brain structures", says Dr. Bruce D. Perry. Tomado de Florencia Barindelli, Carlos G. Gregorio y Lina Ornelas, La protección de datos personales en las redes sociales digitales en particular de niños y adolescentes, IIJusticia/IFAI/IDCR, 2009.

Un estudio de UNICEF indica que 85% de los adolescentes elegirían su computadora o celular con conexión a internet en caso de que se fueran a vivir a otro lugar y sólo pudieran llevar consigo un objeto.[3]

Si bien es cierto que los más pequeños del hogar son los que pueden dominar en minutos cualquier nueva tecnología,[4] también lo es que no por ese hecho cuentan con todas las herramientas emocionales y educativas que los puedan blindar para integrarse de manera armoniosa y segura a una futura ciudadanía digital. Padres y educadores perplejos se sienten impotentes para guiar a las niñas y niños en este nuevo entorno. Por su parte, el Estado intenta desarrollar o adecuar los mecanismos para procurar e impartir justicia, así como cooperar en el ámbito internacional ante el fenómeno de lo "virtual" con el fin de brindar un ámbito de seguridad a los menores.

Podemos aseverar que la humanidad experimentará cambios constantes dada la imparable espiral de innovación, por la que nuevos avances científicos y tecnológicos modificarán, minuto a minuto, la forma en que vivimos. Aunque todavía nos queda mucho por ver, nos encontramos en un momento sin precedentes en lo que se refiere a las posibilidades que nos ofrecen las tecnologías de la información y el conocimiento (en lo sucesivo, TIC), tanto para los individuos en su interactuar diario, como para los gobiernos y las empresas o corporaciones. Cada vez es más común el uso del cómputo en la nube (en inglés, *cloud computing*), el análisis de ingentes cantidades de información (*big data*) o el acceso, así como, en su caso, la reutilización de información pública en el ámbito de gobierno abierto (*open government*), por citar algunas cuestiones de interés.

No obstante, el uso positivo que puede hacerse de las TIC también conlleva peligros o riesgos que, en algunos casos, pueden causar graves daños a los usuarios, como el espionaje de cualquier tipo (comercial o con otros fines), ataques informáticos que incluso puedan llegar a desencade-

[3] <www.slideshare.net/unicefargentina/unicef-argentina-encuestaconsumoadolescentembargado>.

[4] Algunos estudios revelan que cada vez es más común que los niños menores de cinco años no sepan atarse las agujetas de los zapatos, pero sí puede enviar mensajes de texto por un teléfono o cualquier dispositivo móvil.

nar una ciberguerra (*cyberwar*), o los contenidos ilícitos tipo pedofilia,[5] abuso sexual infantil en línea, materiales o contenidos xenófobos y virus, entre otros. Evitar estos riesgos debe ser una corresponsabilidad de todos los actores involucrados, con un especial empoderamiento a los usuarios, de modo que cuenten con los mecanismos para prevenir, en la medida de lo posible, estas amenazas. Dado que más de 30% de la población en México es menor de edad y que cada día la brecha digital se acorta, resulta indispensable contar con una estrategia efectiva en la materia.

Este ensayo tiene como objetivo explorar, de manera general, los impactos positivos y negativos que pueden tener las tecnologías de la información y el conocimiento; intenta dar luz sobre algunos riesgos concretos que se materializan en conductas ilícitas que pueden afectar potencialmente a menores; cuál es el impacto de los medios sociodigitales tales como el internet, la telefonía celular y las redes sociales digitales; la importancia que tiene la protección de los datos personales: sus principios y derechos; las premisas para garantizar de mejor manera la privacidad de los menores y su exposición pública; recomendaciones para que los múltiples actores involucrados se coordinen de cara a una política pública de protección de menores en la era digital, que contenga un adecuado marco normativo, para finalmente concluir abordando el tema educativo como el faro que guíe los esfuerzos de todos los actores involucrados.

El Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal (INFODF) nos encomendó escribir este ensayo para aportar mayores elementos en esta discusión, con la firme convicción de poner en primer lugar a las niñas, niños y adolescentes, de manera que puedan conocer, a través de su derecho a saber y con la ayuda de sus padres, tutores o profesores, información relevante acerca de cómo pueden estar mejor protegidos en plena era digital. Esperamos contribuir a ello.

[5] Al respecto puede verse el comunicado de prensa núm. 34, de la Policía Federal, del 8 de febrero de 2013, en el que anunciaba la detención de un presunto pedófilo en Nuevo León. Véase la noticia en el vínculo electrónico <http://www.ssp.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1266035>.

1. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SU IMPACTO EN LA SOCIEDAD ACTUAL

Sin duda la revolución tecnológica trae consigo ilimitados beneficios a los gobiernos, empresas y personas, facilitando que sus actividades cotidianas sean sencillamente más simples, sin importar la complejidad que encierren las mismas. Sin embargo, de manera paralela a estas bondades, el uso inadecuado de las actuales tecnologías conlleva retos y desafíos a los derechos de las personas, específicamente en su privacidad y en la protección de su información personal.

Sin temor a equivocarnos, es posible afirmar que el novedoso y constante desarrollo de las TIC representa grandes beneficios para los individuos, gobiernos, empresas, corporaciones y sociedad en general. A tal grado que hoy en día vivimos en un mundo multipantalla en el que la mayoría de las actividades que realizamos no las concebimos sin una computadora, *notebook,* teléfono inteligente (*smartphone*), *tablet*, o cualquier otro dispositivo (*gadget*) que podamos conocer o imaginar, y tampoco sin una conexión a internet u otros medios de comunicación electrónica, tales como el correo electrónico o las plataformas de mensajería electrónica.[6]

Los jóvenes han encontrado un espacio ilimitado a su creatividad y para acceder al mundo del conocimiento. Existen fenómenos mundiales a través de los cuales hay niñas y niños que han creado sus propios sitios en internet en los que ayudan a otros a aprender ciencias naturales, matemáticas o física.[7]

[6] Como por ejemplo, Whatsapp, Viber u otras.

[7] Ver sitios como el de KhanAcademy en

Asimismo, organismos internacionales promueven la generación de opiniones críticas de los menores ante temas como sexualidad o violencia.[8] Otros movimientos de la sociedad civil y la industria apoyan la ayuda psicológica a menores que han sido objeto de ciber-bullying u otros delitos, para que puedan compartir experiencias y sentirse menos abrumados y solos ante sus problemas.[9] Las TIC se han convertido en una herramienta de gestión fundamental que ha dado paso a la administración electrónica y, como consecuencia de ello, la relación directa de los ciudadanos con las administraciones públicas se ha visto impulsada a un nuevo nivel, en el que algunas barreras u obstáculos de espacio y tiempo han desaparecido, aunque puedan surgir otros problemas de carácter operativo, tales como la disponibilidad de conexión, el ancho de banda o la disponibilidad del servicio electrónico o de la información.

Un ejemplo de cómo la tecnología ha facilitado la simplificación de los diversos servicios y trámites que ofrece el Gobierno del Distrito Federal a sus habitantes lo encontramos en los llamados Centros de Servicios @ Digital[10] instalados en los diversos centros y plazas comerciales, los cuales son módulos inteligentes (también conocidos como kioscos) que facilitan el pago de servicios y contribuciones de manera cómoda, sencilla, rápida y segura los 365 días del año, como la expedición de copias certificadas del registro civil, el pago de agua, predial, tenencia, permisos de conducir y licencias, derechos de trámites vehiculares, infracciones de tránsito y multas por verificación extemporánea, entre otros servicios.

Otro ejemplo más es el programa e-Seduvi a través del cual la Secretaría de Desarrollo Urbano y Vivienda del Distrito Federal ha logrado la consolidación y entrega de gran parte de sus servicios a través del uso de las comunicaciones electrónicas. Mediante plataformas como Cita en línea, Ciudadmx, Seduvi Site y DROyC, la dependencia ahora es capaz de

<https://es.khanacademy.org>. Asimismo, el sitio de Adora Svitak enseña a los padres y profesores mejores métodos de enseñanza, invirtiendo la regla de que sólo los adultos enseñan a los niños. Ver <www.adorasvitak.com>.

8 <yodigo.org.ar>.

9 Ver It Gets Better Project, en <www.itgetsbetter.org>.

10 Sobre estos Centros de Servicio @ Digital puede verse más información en el vínculo electrónico <http://www.finanzas.df.gob.mx/csDigital/servicios.html>.

ofrecer la posibilidad de realizar citas en línea, consultar el tipo de uso de suelos para el desarrollo de proyectos urbanos vía internet, y mantener un control más robusto de los trámites y su propio ciclo de vida mientras son gestionados con la facilidad de darles seguimiento y con notificaciones automáticas vía correo electrónico cada vez que el trámite cambie de estatus.

Se trata de ejemplos que muestran los avances que se han producido si bien se plantean nuevos retos, tales como la necesidad de autenticación por medios electrónicos sin la presencia física simultánea de las partes, lo que da lugar a la necesidad de hacer uso de la firma electrónica,[11] basada en certificados electrónicos, así como otras cuestiones entre las que se encuentra de manera prioritaria la debida protección de datos personales.

Es la posibilidad de gestionar la administración de manera eficiente lo que nos lleva a la necesidad de tomar en consideración que la información, sea personal o no, en poder de aquélla, deja de ser un bien para convertirse en un servicio (en inglés, *information as a service*).

Además, el uso y aplicación de las TIC en nuestras vidas se concreta en otros ámbitos, como por ejemplo en el campo de la salud a nivel nacional y mundial. En este último caso, por citar un ejemplo, científicos de la Universidad de St. Andrews The London School of Hygiene & Tropical Medicine and NHS Greater Glassgow and Clyne, están probando en Kenia una potencial herramienta llamada *Peek* para la prevención de la ceguera en países de bajos recursos.

Esta novedosa aplicación utiliza la cámara de un teléfono inteligente para comprobar la prescripción de anteojos, diagnosticar cataratas, e incluso examinar la parte posterior del ojo para el diagnóstico de varias enfermedades. En la actualidad, para llevar a cabo una amplia gama de pruebas de diagnósticos oftalmológicos se necesita de una gran cantidad de equipo médico y humano con presupuestos insostenibles para la atención de poblaciones de escasos recursos.

[11] Al respecto, véase la Ley de firma electrónica del Distrito Federal, publicada en la Gaceta Oficial del Distrito Federal del 4 de noviembre de 2009. Disponible en el vínculo electrónico <http://www.poderjudicialdf.gob.mx/work/models/PJDF/Transparencia/IPO/Art14/Fr01/01Leyes/LeyFirmaElectronica_20110816.pdf>.

Esta nueva tecnología pretende obtener valiosa información clínica a bajo costo, a tal grado que una persona no experta podrá manejar. Las pruebas sobre la efectividad de *Peek* se están realizando en 5 000 personas en Kenia y haciendo comparaciones con los equipos tradicionales.[12]

Por otra parte, si hablamos de los beneficios tecnológicos a nivel personal, algunos ejemplos son la multiplicidad de aplicaciones al servicio de los usuarios de *smartphones* (llamadas *apps*) que van desde el acceso a noticias de último momento, conversaciones instantáneas, juegos, estaciones radiofónicas, pasando por la geolocalización, redes sociales, moda y belleza, hasta banco en línea, por mencionar sólo algunas.

Un caso ilustrativo lo encontramos en plena Ciudad de México, donde cualquier persona que viva en esta ciudad, tenga un teléfono inteligente y cuente con la aplicación (*app*) que se requiere, puede solicitar un servicio de taxi desde su celular.

En el caso de las niñas y niños del Distrito Federal, un claro ejemplo de los beneficios de las TIC es el proyecto "Aprende a Aprender con TIC", que integra los niveles de educación básica, primaria y secundaria.[13] A través de dicho proyecto, las niñas y niños del DF, e incluso otros usuarios con conexión a internet desde cualquier lugar de la República o del mundo, pueden acceder a contenidos que les permitirán "conocer, aprender, jugar y compartir".

Con carácter general, el portal está dirigido a la comunidad educativa, incluyendo a padres, docentes y escuelas con el propósito de fomentar el aprendizaje permanente mediante el uso de las TIC.

Dirigido en particular a docentes y escuelas, a través del portal del proyecto es posible acceder al Cuadernillo *Estándares TIC para la Educación Básica en el Distrito Federal*[14] que explica el significado y alcance del

[12] La información completa sobre esta aplicación se encuentra disponible en el vínculo electrónico <http://www.st-andrews.ac.uk/news/archive/2013/title,223732,en.php>.

[13] Sobre este proyecto, puede verse <http://tic.sepdf.gob.mx>.

[14] Disponible en la dirección electrónica <http://tic.sepdf.gob.mx/images/archivos/inicio/estandares_20100622.pdf>.

mismo, y pone a disposición de quienes estén interesados "el conjunto de estándares y estrategias definidos para el uso educativo de las TIC, haciendo énfasis en que no son limitativos de lo que pueden lograr sus alumnos, ni de lo que ustedes, como docentes, pueden enseñar."[15]

Entre las cuestiones que se explican en dicho Cuadernillo cabe destacar el hecho de que se promocione enseñar responsabilidad, lo que se concreta en que "es indispensable que niñas, niños y jóvenes reflexionen críticamente sobre una serie de valores y prácticas", e incluye la siguiente tabla:[16]

- Acceso equitativo a la tecnología.
- Libertad de expresión.
- Criterios de verdad, exactitud y objetividad en el intercambio de información.
- Protección y seguridad en la información.
- Respeto a la intimidad y vida privada de las personas.
- Protección del derecho de autor y de la propiedad intelectual.
- Prácticas honestas en el uso de la información, evitando toda forma de plagio.
- Prácticas responsables, evitar el fomento y distribución de material que perjudica la integridad de otras personas o grupos.
- Prácticas de cuidado de sí mismo.

[15] Página 5 del citado Cuadernillo.

[16] Véase la página 44 del citado Cuadernillo.

Y todos estos ejemplos, así como otros muchos que podríamos apuntar, tienen algo en común: se trata de avances tecnológicos en beneficio de las personas, siempre y cuando se garanticen sus derechos, entre los que se encuentra el derecho fundamental a la protección de datos personales, así como los derechos de terceros, tales como la propiedad intelectual, el derecho a la información o a la libertad de expresión. Estos avances tecnológicos, que en particular deben garantizar la privacidad y la seguridad, evitan intromisiones ilegítimas en la privacidad y la dignidad de las personas, ya sean adultas o menores de edad, y especialmente en este último caso. Sin embargo, de manera paralela a todos los beneficios citados que trae aparejado el constante desarrollo de las TIC para hacer que las actividades gubernamentales, educativas, sociales, económicas, en salud, bancarias y cualquier otra del diario vivir sean más sencillas, accesibles y eficientes, existen riesgos potenciales derivados del uso excesivo, inadecuado e irresponsable de estas tecnologías por parte de sus usuarios.

Al respecto, cada vez más las personas comienzan a ser víctimas de conductas que pueden causar daño en su reputación o en otros bienes o derechos personales o patrimoniales.

El caso más típico es la recepción no deseada y cotidiana, e incluso molesta, de correos electrónicos ofreciendo productos o servicios no solicitados (*spamming*), el cual en algunas veces el envío es masivo y sin consentimiento del destinatario, y en otras ocasiones, este envío masivo se convierte en hipercontextualizado al tomar en cuenta los perfiles e intereses de los destinatarios, pero igualmente sin consentimiento o solicitud previa.

Otro ejemplo de estos riesgos se materializa en el robo de identidad que sufren los usuarios de internet, cuando terceros tienen la facilidad y medios para acceder a contraseñas, número de tarjetas de crédito o débito, cuentas bancarias, identificaciones (tales como el número de la CURP) y cualquier otro tipo de información personal disponible en la red, con la finalidad de obtener recursos económicos virtuales, adquirir bienes o servicios a nombre y cargo de la víctima, o suplantar su identidad en una red social o profesional sin que ésta tenga conocimiento de la operación transaccional o de otra naturaleza que supuestamente realizó. En apartados posteriores vamos a particularizar ciertas conductas ilícitas en línea cometidas contra menores.

2. EL IMPACTO DE LOS MEDIOS SOCIODIGITALES

Internet permite el intercambio de información urbi et orbe, así como el desarrollo de la creatividad y la personalidad de los menores. De manera paralela a los usos y beneficios que nos brinda internet, también existen riesgos que derivan de un uso inadecuado por parte de los usuarios de esta poderosa herramienta. Este apartado analiza también aspectos relacionados con la telefonía móvil y las redes sociales digitales, poniendo en relieve los actos ilícitos que pueden cometerse contra los menores a través de estos medios sociodigitales.

2.1. *Internet: usos y beneficios*

La *world wide web* o internet es definida por Barriuso (2002)[17] como una red de computadoras conectadas entre sí y ubicadas en distintas partes del mundo que permite el intercambio de información, bajo un lenguaje común a todas las máquinas que se conoce como protocolo.

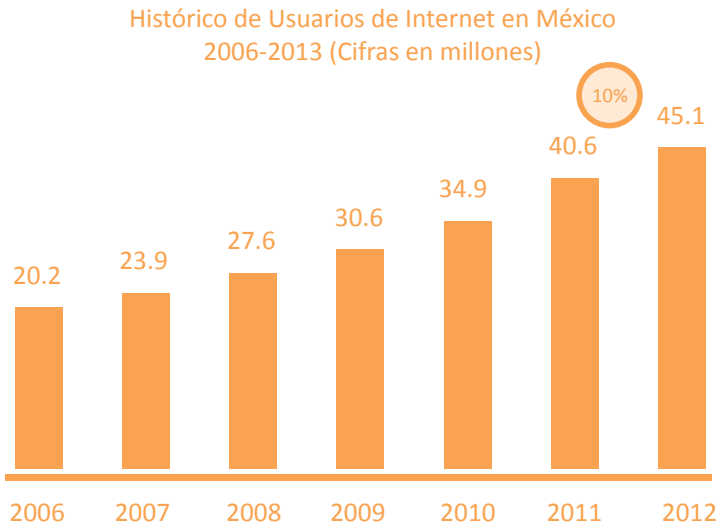
Así, la existencia y evolución de internet ha conformado un espacio virtual que ofrece infinidad de información de todo tipo, donde el usuario ha pasado de ser un "usuario pasivo", esto es, su interacción con internet se acota a acceder o consultar simplemente información sin manifestar sus opiniones o ideas, a convertirse en un "usuario activo" teniendo la posibilidad de crear sus propios contenidos de información y seguir alimentando a la red.

Un ejemplo sencillo de la conversión del usuario a la que hacemos referencia, es que actualmente los usuarios de internet pueden manifestar sus opiniones,

[17] Carlos Barriuso Ruiz, La contratación electrónica, Madrid, Dykson, S.L., 2002, p. 37.

ideas y comentarios sobre las noticias o información que los periódicos publican por esta compleja red, o bien, los usuarios crean sus propios *blogs* con la plena libertad de ser escuchados o más bien leídos y generar debates. Igualmente, usuarios de Facebook, Google+, Linkedin, Twitter u otras plataformas y redes, ponen a diario información, personal o profesional, a disposición de quien quiera leerla.

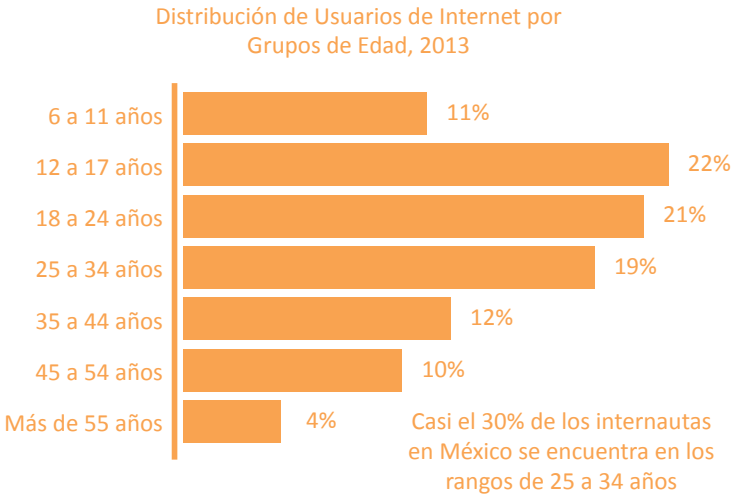
Al respecto, conviene citar las cifras que demuestran el histórico de usuarios de internet en México del año 2006 al 2012, de acuerdo con el *Noveno estudio sobre los hábitos de los internautas en México*[18] elaborado por la Asociación Mexicana de Internet (en adelante, AMIPCI), estudio que aporta las estadísticas más concretas sobre el uso de internet u otros medios de comunicación electrónica equivalentes relativos a menores:



Fuente: Asociación Mexicana de Internet (AMIPCI)

[18] Este estudio se encuentra disponible en el vínculo electrónico <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=348&Type=1>.

De manera más específica, este Noveno Estudio distribuyó a los usuarios de internet por grupo de edad, arrojando la siguiente numeralia:



Fuente: Asociación Mexicana de Internet (AMIPCI)

Según los datos proporcionados por AMIPCI, el 11% de los usuarios de internet tenía entre 6 y 11 años, y el 22% entre 12 y 17 años.

No obstante dichas cifras, ni el sector público, pudiendo citar al respecto al Instituto Nacional de Estadística y Geografía (INEGI), que desde el año 2001 genera información estadística de las Tecnologías de la Información y las Comunicaciones (TIC) en los hogares,[19] o a la Comisión Federal de Telecomunicaciones (COFETEL), ni el sector privado, ofrecen datos detallados relativos al uso de las TIC por los menores, salvo el caso ya citado de AMIPCI, a pesar de que se centra únicamente en el uso de internet.

[19] Al respecto, puede verse la información disponible en <http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp>.

Respecto al 2012, conforme a los datos proporcionados por el INEGI, de "44.7 millones de personas que usaban una computadora; [...] dos de cada tres se agrupaba en el rango de 12 a 34 años de edad". El INEGI también señalaba que "la mayor parte de quienes utilizaban internet se concentró en los jóvenes de 12 a 34 años, con una participación del 64.1%".

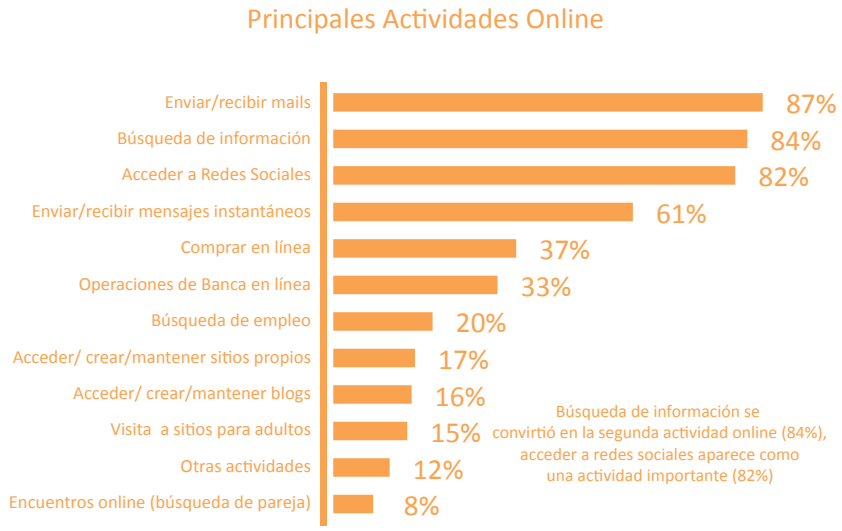
Como sabemos, internet no sólo se reduce al acceso ilimitado de información desde distintas partes del mundo, sino que se ha convertido en una herramienta multifacética; como por ejemplo ser un medio de comunicación personal a través del envío y recepción de correos electrónicos o el uso de comunicación instantánea (*chats*), o en un canal para realizar actividades comerciales como la compra o venta de productos o servicios sin importar la ubicación geográfica donde se encuentren tanto el vendedor como el comprador.

También es un medio de ocio y entretenimiento a través de la publicación de páginas *web* que ofrecen juegos, apuestas y servicios propios de un casino, o videojuegos en línea, música, películas, series, pasatiempos y humor, entre otros ejemplos.

Otra faceta de internet se traduce en ser una fuente inagotable de conocimientos, como por ejemplo la posibilidad de leer libros en línea (*ebooks*), o el acceso a la educación a distancia que ofrecen diversas instituciones educativas a nivel mundial, o en su caso, la impartición de cursos en línea sobre cualquier temática.

Ahora bien, un uso de internet que resulta importante citar por el impacto que ha causado a los menores de edad y a la sociedad en general, es el surgimiento, proliferación y predilección de las redes sociales, de tal modo que las mismas han revolucionado los esquemas tradicionales de socialización a nivel mundial.

Para conocer las principales actividades *on line* que llevan a cabo los mexicanos en internet, de acuerdo con el Noveno Estudio de AMIPCI, a continuación se muestra la siguiente estadística:



Fuente: Asociación Mexicana de Internet (AMIPCI)

De manera paralela a los usos y beneficios que nos brinda internet, también existen riesgos que derivan de un uso inadecuado por parte de los usuarios de esta poderosa herramienta, mismos que la extinta Secretaría de Seguridad Pública Federal (2012) identificó en la *Guía del Taller Prevención contra el delito cibernético*,[20] que citaremos a continuación:

[20] El texto completo de la Guía del Taller Prevención contra el delito cibernético se encuentra disponible en el vínculo electrónico <http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1214152//archivo>.

1. Acceso a la información	El fácil acceso a una gran variedad de páginas, distrae al usuario de su objetivo inicial.
2. Tipo de información	Los usuarios pueden tener acceso a información inadecuada, agresiva, ilícita, pornográfica o xenófoba, entre otras.
3. Relaciones personales	Puede crear un entorno que facilita comportamientos desinhibidos y dar una imagen que no corresponde con la realidad. El uso excesivo puede generar un problema de socialización en las niñas, niños y jóvenes que fomenta el aislamiento.
4. Se puede producir una pérdida de intimidad	La participación en determinados foros, chats y redes sociales requieren que el usuario facilite datos personales a terceros o páginas falsas.
5. Amistades "no convenientes"	El uso de programas de mensajería instantánea y redes sociales permite el contacto con personas desconocidas, que pueden ser violentas y con intenciones ilícitas.
6. Adicciones	El uso excesivo de internet puede provocar "adicción"; sin embargo, ésta dependerá de su perfil, circunstancias personales y situaciones de comportamientos compulsivos.
7. Relativos al propio funcionamiento en internet	Internet no siempre es una red segura, ya que existen sitios web clonados y páginas con un gran número de *spam* y vínculos de sitios web que contienen información inapropiada.
8. Temas económicos	La facilidad para poder ingresar a sitios con miles de servicios y promociones falsas, pueden llevar a los usuarios a ser víctimas de engaños, fraudes, estafas, compras y negocios ilegales, etcétera.

2.2. La telefonía móvil: bondades y riesgos

Citando a la *Guía del Taller Prevención contra delitos cibernéticos* el teléfono móvil, también conocido como celular, es un dispositivo portátil de comunicación inalámbrica el cual no requiere conexión directa a una red fija. Su invención se remonta al siglo XIX y ha adoptado características conforme al avance de la tecnología, algunas de éstas son:

- SMS (*Short Message Service*): es un servicio de mensajería a través del cual se pueden enviar o recibir mensajes entre celulares y otros dispositivos electrónicos, incluso utilizando internet.

- Correo electrónico (*e-mail*): sistema que permite el intercambio de mensajes entre ordenadores conectados a una red.

- GPS (*Global Positioning System*): sistema de navegación y geolocalización mediante satélites.

- Internet: los teléfonos inteligentes cuentan con el servicio de Internet, permitiendo al usuario estar conectado 24 horas al día los 7 días de la semana.

- Videograbación: se puede grabar cualquier situación con alta definición.

- MP3: que permite el almacenamiento de una gran cantidad de música en el dispositivo móvil.

- Juegos: con las aplicaciones específicas se puede jugar *on line*.

El teléfono celular inteligente ha proporcionado a sus usuarios notables beneficios relacionados con la comunicación, socialización, ocio y entretenimiento, entre otros; sin embargo, su mal uso puede acarrear algunas de las siguientes consecuencias:

- La realización de acciones de espionaje con el propio dispositivo.

- La facilidad para realizar conductas antisociales, e incluso, ilícitas.

- La adicción al dispositivo.

- El acceso a y difusión de contenidos inadecuados, por ejemplo, pornográfico o ilícitos, tales como los xenófobos.

De nuevo, el uso que se haga de las TIC, en este caso la telefonía móvil, está en nuestras manos pudiendo citar múltiples ejemplos del sector privado que tienen por objeto, de manera específica, ofrecer información dirigida a padres y menores para que hagan un uso seguro.[21]

[21] A modo de ejemplo pueden verse los consejos que da Telefónica México (Movistar), una de las operadoras de telefonía móvil, a través del vínculo electrónico <http://www.telefonica.com.mx/RC-Sostenibilidad-Como-se-utilizan-las-TIC-Uso-Responsable>. También Google ofrece a sus usuarios una guía para mantenerse seguro y protegido en línea (Good to know), disponible en el vínculo electrónico <http://www.google.com.mx/goodtoknow>.

2.3. Las redes sociales digitales: las razones de su popularidad y los riesgos que conlleva su uso inadecuado

El surgimiento y la actividad en las redes sociales digitales han cambiado drásticamente los esquemas de socialización adoptados y heredados de generación en generación. Así, nuestros abuelos solían convivir en aquellas plazas públicas de cada localidad al aire libre; nuestros padres lo hacían en fiestas o reuniones donde el atractivo principal eran los grupos musicales que tocaban en vivo; a nosotros nos tocó el *boom* de los grandes centros comerciales con restaurantes, tiendas de todo tipo, áreas de comida rápida y espacios apropiados para convivir e interactuar de persona a persona. Y nuestros hijos socializan a través de las redes sociales digitales,[22] de modo que actividades como ir a comer hamburguesas o jugar en el parque con los amigos, han pasado a un segundo plano, ya que gran parte de su vida social es virtual.

Hemos pasado de un entorno reducido y, en cierta medida controlado, como podía ser la plaza pública, a un entorno mundial, ya que ahora nuestro interlocutor o los destinatarios de nuestros mensajes en una red social pueden estar en cualquier lugar del mundo.

Este abrupto cambio de paradigmas de convivencia social quedó reflejado en el Noveno Estudio de la AMIPCI, al concluir que en 2013 el tiempo promedio de conexión diario del internauta mexicano es de 5 horas 1 minuto, lo que supone 67 minutos más que en 2012, y donde el 82% de los 7077 entrevistados manifestó que su tercera actividad favorita en internet es el acceso a las redes sociales, resultando como principales usos el enviar y recibir correos electrónicos, y buscar información, respectivamente.

Pero, ¿qué es una red social? Boyd & Ellison (2007)[23] definen a la red social como un servicio que permite a los individuos:

[22] En material de protección de datos en la redes sociales, véase a José Luis Piñar Mañas y otros autores en Redes sociales y privacidad del menor, España, Reus, 2011.

[23] D.M. Boyd & N.B. Ellison, "Social Network Sites: Definition, History, and Scholarship", Journal of Computer-Mediated Communication, 13(1). El texto completo de este artículo se encuentra disponible en el vínculo electrónico <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

- Construir un perfil público o semipúblico dentro de un sistema delimitado.

- Articular una lista de otros usuarios con los que comparten una conexión.

- Ver y recorrer su lista de las conexiones y de las realizadas por otros dentro del sistema.

Y, ¿en qué radica la popularidad de las redes sociales? Pensamos que son tres las principales razones que hacen que las redes sociales sean muy socorridas por los menores y mayores internautas en la actualidad, a saber:

a) El acceso a las redes sociales es gratuito siguiendo un sencillo ritual: *paso 1*, contar con una computadora fija o móvil, *smartphone*, *tablet*, o cualquier otro *gadget* similar; *paso 2*, tener conexión a internet (a través de un plan tarifario, prepagado o conexión Wi-Fi); *paso 3*, crear un perfil que te describa; *paso 4*, invitar a amigos, conocidos y desconocidos a ser parte de tu propio espacio virtual; y *paso 5*, alimentar (*postear*) con información personal y de terceros este complejo tejido de relaciones que se va formando con la interacción cotidiana.

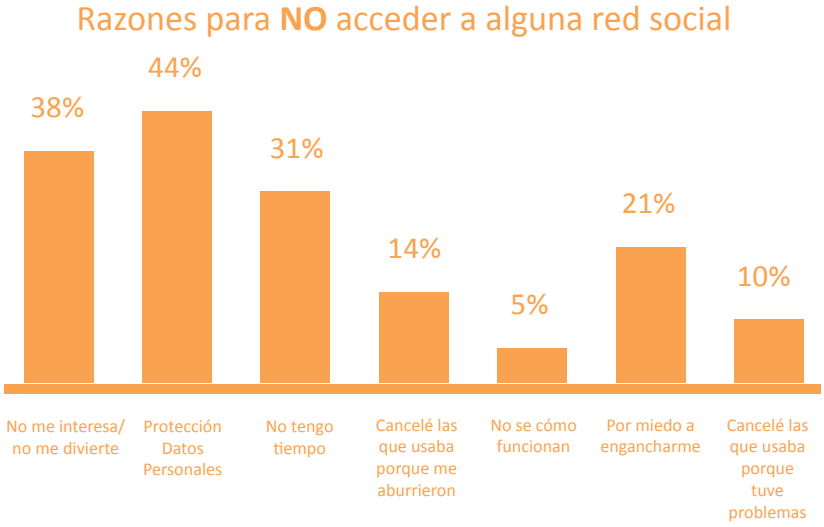
b) Las redes sociales se han constituido en ciberforos de expresión personalísimos, donde los menores y usuarios en general, ejerciendo su derecho a la libertad de expresión y sin inhibición alguna, pueden ser, decir, opinar e incluso soñar quién quiere ser. No por nada, en la mayoría de la información de los usuarios se muestra la faceta más favorable de éstos: viajes, fiestas, mensajes de amistad o amor, éxitos, entre otros aspectos. Casi nadie, por ejemplo, comparte con sus amigos el regaño de mamá o del jefe, o las deudas pendientes de liquidar, tratándose de adultos.

c) Las redes sociales permiten conocer y convivir virtualmente con personas de cualquier parte del mundo que comparten los mismos gustos, aficiones, intereses y forma de pensar. Es decir, en

especial los menores creen sentirse realmente identificados con otras personas, y en cierto modo comprendidos, valorados, apoyados y aceptados tal cual son por sus amigos virtuales.

Este efecto viral del que hablamos se refleja en el multicitado Noveno Estudio de la AMIPCI, al señalar que el 93% de los 7077 entrevistados sí hacen uso de las redes sociales, mientras que el 7% de los entrevistados no interactúan en las mismas; esto es, 9 de cada 10 internautas mexicanos accede a alguna red social.

Asimismo, conviene citar las razones de los 524 entrevistados que no pertenecen a alguna red social:



Fuente: Asociación Mexicana de Internet (AMIPCI)

Finalmente, queremos cerrar este apartado señalando que este efecto viral de las redes sociales no sólo se acota a sus usuarios como individuos (menores o adultos), sino que el uso de las mismas ha revolucionado los modelos de negocios actuales, ya que las personas jurídicas como las empresas, instituciones públicas y organizaciones de la sociedad

civil, se han dado a la tarea de valerse de estas plataformas sociales para posicionar sus marcas, productos y servicios.

El *Segundo estudio sobre redes sociales en México* de la AMIPCI (2012)[24] arrojó que 83% de las 206 empresas encuestadas sí hace uso de las redes sociales, mientras que 17% restante no lo considera necesario o no tiene personal calificado para el manejo de perfiles sociales. Esto es, 8 de cada 10 empresas evaluadas poseen algún perfil social.

De manera complementaria, este segundo estudio identificó las redes sociales más utilizadas por las 206 empresas encuestadas, como lo muestra la siguiente gráfica:

Fuente: Asociación Mexicana de Internet (AMIPCI)

[24] El estudio se encuentra disponible en el vínculo electrónico <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=198&Type=1>.

Un ejemplo de esta actual revolución que vienen presentando los modelos de negocios tradicionales, lo encontramos en un nuevo modelo crediticio que mediante la combinación de técnicas basadas en métodos microfinancieros, más la cantidad de datos existentes en las redes sociales y la reputación que el solicitante tenga en los medios en línea, se otorgan préstamos a aquellas personas que no tienen acceso a servicios y productos bancarios.

El punto central de este modelo radica en que la obtención del crédito se realiza en función de la reputación que el solicitante tenga en las comunidades virtuales como Facebook, Linkedin, Google y Yahoo!

Es así como millones de usuarios de las redes sociales a nivel mundial se han convertido en adeptos y aficionados de estas comunidades virtuales para los distintos fines que persiguen, como puede ser entretenimiento, conocimiento, socialización, comunicación instantánea, comercial u otros, haciendo uso de la variada gama de aplicaciones, innovaciones y posibilidades que ofrecen.

Por otro lado, el uso de las redes sociales ha penetrado tanto en la vida de sus adeptos, que hay personas que no dan un paso en su vida, por más trivial o importante que sea, sin *postearlo* y, por consiguiente, inmortalizarlo en éstas. A tal grado que estas plataformas virtuales no sólo se han convertido en una herramienta para conectar a las personas, sino en una extensión de la personalidad de los usuarios, lo cual, dependiendo de la información divulgada, puede favorecer o perjudicar al usuario a corto, mediano o largo plazo.

Al respecto, el estudio *Digital records could expose intimate details and personality traits of millions*, realizado por la Universidad de Cambridge y Microsoft Research Cambridge (2013),[25] demostró que a través de los *likes* (gustos o preferencias) que postean en Facebook los usuarios cuando les gusta o aprueban algo, puede inferirse, asombrosamente con cierta precisión, información personal más íntima del usuario

[25] Los resultados y conclusiones completas del estudio se encuentran disponibles en el vínculo electrónico <http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions>.

como su raza, edad, coeficiente intelectual, sexo, personalidad, consumo de drogas y afiliación política.

Los investigadores de Cambridge´s Psychometrics Centre y de Microsoft Research Cambridge analizaron simple y sencillamente los *likes* de aproximadamente 58 000 usuarios de Facebook en Estados Unidos, a partir de los cuales crearon un perfil psicológico de cada participante.[26]

Sorprendentemente, los algoritmos utilizados en este estudio alcanzaron los siguientes niveles de exactitud:

Porcentaje de exactitud	Información personal identificada
88%	El género masculino de los participantes.
95%	La raza de los participantes: afroamericanos o blancos.
82%	La religión que profesan los participantes: cristianos o musulmanes.
85%	La afiliación política de los participantes: republicanos o demócratas.
65 al 73%	El estado civil de los participantes y el consumo de drogas.

Por su parte, el investigador David Stillwell, de la Universidad de Cambridge, señaló que él es usuario de Facebook desde 2005 y lo seguirá siendo; sin embargo, tendrá más cuidado sobre su perfil de privacidad.

Otro ejemplo sobre el acceso exponencial e incontrolable a la información personal que se publica en las redes sociales, lo encontramos en aquellos casos de personas que han sido rechazadas por un futuro empleador después de acceder y conocer información, videos o fotografías del candidato en cuestión en situaciones comprometedoras o “alegres”.

[26] Sobre las conclusiones de este estudio, Thore Graepel, de Microsoft Research, manifestó que deseaba que el estudio contribuyera a la discusión en torno al tema de la privacidad, donde los usuarios esperan que la industria implemente medidas y controles de seguridad más estrictos desde el desarrollo de los productos y servicios que ofrece; por su parte, los usuarios de Facebook deben tener más cuidado sobre la información que comparten, su perfil de privacidad y no compartir información con extraños.

Concretamente, los riesgos en el caso de menores los podemos identificar con lo señalado por Peschard (2011):[27] "Esta exposición constante y pública de la información en las redes sociales que implica ciertos peligros, es particularmente importante cuando es relativa a los menores de edad porque pueden acceder a contenidos de información que no son pertinentes para su edad o entrar en contacto con personas que explotan su información; esa información que circula con gran fluidez pudiendo ser objeto de discriminación, de difamación, de violencia psicológica e incluso acoso sexual o pornografía. Todos estos riesgos pueden dañar el desarrollo integral del niño y del adolescente."

Aunado a los riesgos a los que están expuestos los menores de edad citados por la doctora Peschard en las redes sociales, como son difamación, discriminación, violencia psicológica, acoso sexual y pornografía, se suman otros como el *ciberbullying* y *cibergrooming*.

De acuerdo con la citada *Guía del Taller Prevención contra delitos cibernéticos*, el *ciberbullying* se da entre menores y se define como los insultos, humillaciones, amenazas y chantaje, entre otras ofensas, a través de un dispositivo tecnológico; agresiones virtuales que se distinguen por lo siguiente:

Actores involucrados:	Existe una víctima, uno o varios agresores y miles o millones de espectadores debido al alcance de los medios tecnológicos.
Contexto aplicable:	Se da en la realidad virtual.
Tipo de afectación:	Al no existir contacto personal, la violencia es psicológica o social.
Identificación del agresor o agresores:	El agresor puede quedar en el anonimato.
Periodicidad de las agresiones:	Las agresiones se mantienen constantes, las imágenes, videos o comunicados afectan a la víctima no sólo cuando son posteadas, sino cuando una persona y otra, y otra, y otra y otra y así hasta contabilizar cientos, miles o millones de personas, tienen acceso a las mismas; es decir, las agresiones son permanentes mientras se mantengan expuestas en el ciberespacio.

[27] J. Peschard (2011), "Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos", en Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes, Memorandum de Montevideo, Instituto de Investigación para la Justicia/Instituto Federal de Acceso a la Información y Protección de Datos, p. 22.

Esta misma Guía señala que el *cibergrooming* consiste en el conjunto de estrategias que una persona adulta utiliza para ganarse la confianza del menor a través de internet con el objetivo de conseguir concesiones de índole sexual, ya sea el envío de fotos o videos, o mantener un contacto físico.

A continuación se describen puntualmente los pasos que llevan a cabo este tipo de personas para lograr sus objetivos:[28]

Empatía	Crea empatía con la mayoría de las actividades que realiza la víctima, logrando que se sienta cómodo para obtener su confianza.
Vínculo	Desarrolla intimidad con el/la menor de tal manera que lo convence de una amistad, de una relación de pareja o hermandad.
Obtención de información	Sirviéndose del vínculo establecido, el ciberacosador rebasa los límites de la confianza, pidiendo información más comprometedora o reveladora, y sugiere que la/el menor que realice acciones eróticas con partes de su cuerpo ante la *webcam*, las cuales servirán posteriormente para chantajearlo o forzarlo a citarse con el acosador en algún lugar.
Intimidación	Obteniendo el primer material de video, fotográfico o escrito, el ciberacosador amenaza a la víctima con la exposición del material a su círculo social, lo que va mermando emocional y psicológicamente a la víctima.
Encuentro físico	Finalmente, el ciberacosador consigue encontrarse con su víctima para efectuar el ilícito.

Otro riesgo que consideramos necesario mencionar es el *sexting*, palabra tomada del inglés que une *sex* (sexo) y *texting* (envío de mensajes de texto vía SMS desde teléfonos móviles). Sin embargo, el desarrollo de los teléfonos móviles ha permitido que el término también englobe el envío de fotografías y videos.

[28] Este modelo fue desarrollado por Erick Stephens, exdirector nacional de tecnología de Microsoft México.

Sus características principales son las siguientes:

- El protagonista posa en situación erótica o sexual.

- El material de texto, fotográfico o de video es producido de forma voluntaria por el mismo autor, quien lo transmite a través del celular.

Relacionado con el *sexting*, existe otro fenómeno llamado *sexcasting* que consiste en la grabación de contenidos sexuales a través de la *webcam* y la difusión de los mismos por correo electrónico, redes sociales o cualquier canal que permitan las nuevas tecnologías.

Esta actividad no genera un daño en el momento de la producción a los autores; sin embargo, sí causa consecuencias negativas posteriores, como las siguientes:

Amenazas a la privacidad del menor:	Cuando el material es visto por cualquier persona.
Daño psicológico:	Cuando la difusión del material provoca que al autor se le someta a maltrato y humillaciones, causando problemas de ansiedad, depresión, exclusión social o suicidio.
Sextorsión:	Cuando el material cae en manos de una persona que lo utiliza para extorsionar o chantajear al protagonista de las imágenes o videos.
Riesgo de geolocalización:	Cuando las aplicaciones de geolocalización y geoetiquetado de contenido multimedia para dispositivos móviles pueden facilitar la ubicación física de las personas.

Desafortunadamente, de no existir suficiente información en los jóvenes, cada día se producen casos que se han difundido públicamente, como el de Amanda Todd, una adolescente canadiense que fue víctima de difamación, discriminación, *ciberbullying*, violencia psicológica y otras conductas transgresoras de su intimidad, personalidad y seguridad a través de las redes sociales, quien ante una severa depresión que presentaba terminó por quitarse la vida.

Antes de este fatal desenlace, Amanda publicó un video en YouTube[29] en el que no habla pero a través de papeles escritos por ella, cuenta los sucesos que la llevaron a acabar con su vida.

Debido al efecto viral de las redes sociales, así como a la computación ubicua, las agresiones, la violencia psicológica, el acoso, la difamación, e incluso la violencia física nunca cesaron para Amanda, a pesar del transcurso del tiempo y de haberse cambiado de domicilio.

Desafortunadamente esta escalofriante historia expone puntualmente los riesgos a los que están expuestos los menores en el ciberespacio y lo frágiles y vulnerables que se vuelven para manejar y controlar este tipo de situaciones, debido a su escaso grado de madurez y a que están en pleno proceso de reconocimiento de su propia identidad y desarrollo de su personalidad, llegando al extremo de tomar decisiones como quitarse la vida al considerar que ésta ya no tiene sentido o futuro.

Por último, en este apartado queremos hacer referencia a las reflexiones que el profesor Rodotá (2011)[30] ha identificado en torno a la privacidad del menor en las redes sociales, resaltando la necesidad de replantear el concepto tradicional de privacidad con el objetivo de obtener mejores garantías de seguridad o protección para el menor sobre la información a la que tiene acceso (entrante) a través de herramientas como filtros, software e incluso la propia privacidad por diseño *(privacy by design).*[31]

---

29 El video se encuentra disponible en el vínculo electrónico <http://www.youtube.com/watch?v=Pc1sK1WX2LA>.

30 S. Rodotá (2011), "Sociedad contemporánea, privacidad del menor y redes sociales", en Redes sociales y privacidad del menor, Madrid, Fundación Solventia, p. 39.

31 La privacidad por diseño es una práctica que ha permitido conciliar, por una parte, los requerimientos de seguridad exigidos en las legislaciones nacionales o estándares internacionales, y por el otro, garantizar una efectiva protección de la información tratada en la consecución de políticas públicas o modelos de negocios. La privacidad por diseño parte de la premisa de que la privacidad no puede ser concebida como un cumplimiento legal, sino más bien como una buena práctica que por defecto debe estar presente desde la concepción y diseño de cualquier política pública, modelo de negocio, aplicación, sistema de información o tecnología que implique el tratamiento de datos personales. Para mayor información al respecto, se sugiere consultar el vínculo electrónico <http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD>.

Rodotá resalta también la necesidad de equilibrar el interés y el bienestar del menor, para evitar caer en un exceso de paternalismo que puede ser un tipo de intervención que limita la idea misma de autonomía del menor.

Al respecto, Rodotá menciona que:

> Al plantear la cuestión desde la perspectiva del libre desarrollo de la personalidad, si el menor está convencido de que la dimensión racional es la prohibición, habrá un problema de desarrollo de la personalidad en la dimensión de la autonomía, que es un punto capital en el libre desarrollo de la personalidad.
>
> Y existe también el riesgo de que una orientación prohibicionista directa, agresiva y no persuasiva pueda producir la llamada "atracción del fruto prohibido". Para un menor, una prohibición se convierte inmediatamente en curiosidad, y debe tener una respuesta.
>
> La indicación puramente negativa de un sitio web puede hacer que, desde el momento de la prohibición, lo convierta en más interesante que los otros para el menor. Éste es un tipo de reacción emocional que debemos tener en cuenta.

Lo que Rodotá desaconseja es afrontar el problema de la protección de los menores en las redes sociales desde un punto de vista negativo, ya que las redes sociales son un medio de transparencia positiva de los fenómenos sociales. Lejos de prohibirles a los menores dejar una red social, debe acompañársele y brindarle todo tipo de información sobre las consecuencias de su actuar.

Por último, enfatiza la necesaria participación de todos los actores interesados sobre los problemas vinculados a los aspectos negativos y riesgos de las redes sociales e Internet 2.0, con la finalidad de desarrollar todas las oportunidades y potencialidades ofrecidas por esa nueva dimensión de internet.

3. EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Las primeras aproximaciones al derecho a la protección de datos Personales, devienen del reconocimiento del derecho fundamental a la vida privada y familiar. En las últimas cuatro décadas han aparecido un gran número de descubrimientos y avances tecnológicos que han coadyuvado a mejorar la calidad y condiciones de vida de la sociedad en general, por ejemplo, la portabilidad del expediente clínico y la telemedicina, entre otros.

Sin embrago, la rápida evolución tecnológica plantea nuevos retos desde la perspectiva de los derechos de las personas, específicamente con el derecho a la protección de los datos personales, precisamente porque las tecnologías presentes facilitan el acceso, transferencia, explotación y almacenamiento de una gran cantidad de información, incluyendo aquella que identifica o hace identificable a los individuos.

Por lo anterior, se hizo necesario reconocer un nuevo derecho fundamental que dotara al titular de los datos de un medio para garantizar la disposición y control de su información personal, denominado derecho a la protección de datos personales o autodeterminación informativa. Este derecho debe evolucionar en la era digital para su mayor eficacia.

3.1. Su origen, naturaleza y alcance

El origen de las leyes sobre protección de datos personales, a nivel internacional, se remonta a la década de 1970, tanto en la Unión Europea[32] como en Estados Unidos.[33] También en el ámbito internacional, Incluso unos años antes, en 1968, el Consejo de Europa adoptó su Resolución 509 de la Asamblea del Consejo de

[32] Por lo que se refiere a los países de la Unión Europea, ya que entonces no existía todavía ésta como tal, es posible citar que durante esos años se promulgaron leyes sobre protección de datos en Alemania, Francia, Dinamarca y Luxemburgo.

[33] En concreto, véase la Ley de Privacidad de 1974 (The Privacy Act of 1974, Pub. L. 93-579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 522a).

Europa sobre derechos humanos y nuevos logros científicos y técnicos,[34] en la que ya se pronunciaba sobre la necesidad de analizar los avances tecnológicos a la luz del derecho a la privacidad reconocido en el artículo 8 del Convenio Europeo sobre Derechos Humanos,[35] de tal forma que en un principio estuvo enfocado a garantizar la protección de la intimidad de las personas en relación con el desarrollo de las TIC, a las que se veía con cierta desconfianza.

Posteriormente, en el caso de la Unión Europea, la referencia a la intimidad ha evolucionado de manera que actualmente se habla ya de un derecho fundamental autónomo, pudiendo citar al respecto tanto la Directiva 95/46/CE[36]

[34] Disponible, en inglés, en la dirección electrónica <http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta68/EREC509.htm>.

[35] El citado artículo consagra el derecho al respeto a la vida privada y familiar en los términos siguientes:
Artículo 8. Derecho al respeto a la vida privada y familiar.
1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.
El Convenio está disponible en la dirección electrónica <http://www.echr.coe.int/Documents/Convention_SPA.pdf>.

[36] Directiva 95/46/CE del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, publicada en el Diario Oficial de la Unión Europea L 281, del 23 de noviembre de 1995. Se trata de la norma general en protección de datos personales en la Unión Europea, ya que en el sector de las comunicaciones electrónicas hay una norma específica, la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, del 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), publicada en el Diario Oficial de la Unión Europea L 201, del 31 de julio de 2002. Esta última Directiva ha sido modificada en varias ocasiones: primero por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, del 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, publicada en el Diario Oficial de la Unión Europea L 105, del 13 de abril de 2006, y después por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, del 25 de noviembre de 2009, publicada en el Diario Oficial de la Unión Europea L 337, del 18 de diciembre de 2009.

y, finalmente, la Carta de Derechos Fundamentales de la Unión Europea,[37] que en su artículo 8 consagra el derecho fundamental a la protección de datos personales, indicando lo siguiente:

> Artículo 8. Protección de datos de carácter personal.
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Se reconoce así el derecho fundamental a la protección de datos personales como un derecho autónomo.[38]

---

[37] Publicada en el Diario Oficial de la Unión Europea C 364, del 18 de diciembre de 2000 y disponible en la dirección electrónica <http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

[38] A nivel nacional, por citar un ejemplo, en el caso de España, la autonomía de este derecho ha sido también reconocida por el Tribunal Constitucional, que en su sentencia 292/2000, del 30 de noviembre, por la que se resuelve el recurso de inconstitucionalidad 1.463/2000 respecto de los artículos 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999 del 13 de diciembre, de Protección de Datos de Carácter Personal, señaló que:
[...] el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, usos posibles por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. (Fundamento Jurídico séptimo).
El texto completo de la Sentencia está disponible en el vínculo electrónico

A nivel nacional, el reconocimiento del derecho fundamental a la protección de datos personales es más reciente, a pesar de que en el sector público hay normatividad tanto federal como estatal desde hace varios años.

En concreto, fue en 2009 cuando se reformó la Constitución en dos ocasiones para, por una parte, establecer la facultad expresa del Congreso para legislar en materia de protección de datos personales en posesión de los particulares[39] y, por otra parte, se modificó el artículo 16 constitucional, incorporando el derecho de toda persona a la protección de su datos personales, así como sus derechos de acceso, rectificación, cancelación y oposición.[40]

Como consecuencia de dichas reformas, en el *Diario Oficial de la Federación* del 5 de julio de 2010, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[41] (en adelante, LFPDPPP). Dicha ley vino a dar respuesta a los compromisos que México había adquirido en diferentes foros internacionales, alineándose con otros países que ya contaban con legislación sobre la materia. Incluso, "una vez más México se pone a la cabeza de los países de América Latina que cuentan con ley de protección de datos, como son Argentina, Uruguay, Colombia, Perú, Nicaragua, Costa Rica y poco más."[42]

<http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=13751>.

39 Se trata del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación del 30 de abril de 2009. El Decreto puede verse en el vínculo electrónico <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf>.

40 Véase el Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación del 1 junio de 2009. El Decreto puede verse en el vínculo electrónico <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf>.

41 Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en el vínculo electrónico <http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010>.

42 Véase José Luis Piñar Mañas y Lina Ornelas Núñez, "Los principios de la protección

Y en el sector público, hay que tomar en consideración, a nivel federal, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental [43] y, a nivel del D.F., la Ley de Protección de Datos Personales para el Distrito Federal[44]. Estas normas, en sus respectivos ámbitos de competencia, rigen el tratamiento de datos personales en posesión de los sujetos obligados del sector público.[45]

De esta manera, el derecho a la protección de datos personales se erige como *el poder de disposición y control que faculta a su titular a decidir cuáles de sus datos proporciona a un tercero, así como el saber quién posee esos datos y para qué, pudiendo oponerse a esa posesión o uso*, constituyéndose un nuevo derecho fundamental con su propio contenido y mecanismos para su pleno ejercicio.

Por tanto, con independencia de que los datos personales sean tratados por un sujeto obligado del sector público o del sector privado, ya sean responsables o encargados del tratamiento, el titular de los datos personales, que es la persona física a la que se refieren los mismos, tiene reconocido este derecho fundamental así como los derechos de acceso, rectificación, cancelación y oposición, conocidos también como "derechos ARCO".

Antes de continuar con la exposición de los aspectos relevantes del derecho fundamental a la protección de datos personales y, por lo que se refiere a su alcance, es necesario que las diferentes partes de este derecho sean conscientes de sus obligaciones y de las implicaciones que tiene el mismo.

---

de datos personales", La protección de datos personales en México, México, Tirant lo Blanch, 2013.

43 Publicada en el Diario Oficial de la Federación del 11 de junio de 2002. Disponible en el vínculo electrónico <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>.

44 Publicada en la Gaceta Oficial del Distrito Federal del 3 de octubre de 2008. El texto de la ley se encuentra disponible en el vínculo electrónico <http://www.infodf.org.mx/nueva_ley/14/1/doctos/LPDPDF.doc>.

45 En el ámbito federal, es necesario tomar también en consideración los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación del 30 de septiembre de 2005. Se encuentran disponibles en el vínculo electrónico <http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf>.

Desde el punto de vista del titular de los datos personales, es necesario que sea consciente de que es titular de un derecho fundamental y de que sus datos personales tienen un valor[46] vinculado a su privacidad y dignidad. Ser titular del derecho fundamental también conlleva ciertas obligaciones, tales como informarse de a quién y para qué le da su consentimiento en caso de que éste sea necesario, así como con qué finalidad van a ser tratados sus datos personales.[47]

Especialmente, cuando navegamos por internet y descargamos una *app* en nuestro celular o *tablet*, es importante leer el aviso de privacidad, así como los términos o condiciones de uso.

Por ejemplo, lo primero que habría que ver cuando accedemos a una página o sitio web al que vayamos a proporcionar nuestros datos personales es si el mismo está sujeto o no a la normatividad sobre protección de datos personales y, en cualquier caso, para qué necesitan nuestros datos personales, durante cuánto tiempo y si podemos ejercer nuestros derechos ARCO.[48] Es decir, se trata de que el titular de los datos personales se informe de quién, cómo y para qué se van a tratar sus datos personales, lo que en el caso de los menores puede requerir del consejo de sus padres o tutores legales.

Y desde el punto de vista del sujeto obligado que trata datos personales, tiene que adoptar las medidas necesarias para cumplir con la normatividad

[46] En relación con el valor de los datos personales, puede verse Study on monetising privacy. An economic model for pricing personal information, European Union Agency for Network and Information Security (ENISA), 28 de febrero de 2012. Este estudio está disponible, en inglés, en el vínculo electrónico <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport>.

[47] Sobre el significado del derecho fundamental a la protección de datos personales, puede verse también Tu derecho a la privacidad: la protección de tus datos personales, Colección Educación Cívica, núm. 4, InfoDF. Disponible en el vínculo electrónico <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/tuderechoalaprivacidad/derechoalaprivacidad.pdf>.

[48] Sobre la protección de datos personales online, puede verse el Documento de trabajo del Grupo de Trabajo de la Directiva 95/46/CE titulado Privacidad en Internet: enfoque comunitario integrado de la protección de datos en línea, WP 37, adoptado el 21 de noviembre de 2000. Disponible, en español, en el vínculo electrónico <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_es.pdf>.

y garantizar el derecho fundamental a la protección de datos personales de los titulares de los datos personales. En especial, si pensamos en un responsable del sector privado que trata datos personales de menores, éste tendrá que adoptar medidas específicas si aquéllos son relativos a menores, ya que en virtud de los Lineamientos del Aviso de Privacidad,[49] deberá considerar incluir en el aviso de privacidad integral, como buena práctica:

- Los mecanismos para recabar el consentimiento de quien ejerza su patria potestad o, en su caso, su tutor o representante legal.

- Las acciones, medidas y previsiones especiales que haya adoptado el responsable en relación con estos tratamientos.

En definitiva, el derecho fundamental a la protección de datos personales se concreta en un poder de disposición y control por el titular de los datos sobre el uso que haga de los mismos el responsable del tratamiento, de manera que este último tiene que adoptar medidas para cumplir con la normatividad que le es exigible y, en particular, considerar los tratamientos de menores u otras personas en supuestos de interdicción o que tengan necesidades específicas.

[49] En concreto, el Lineamiento cuarto indica lo siguiente:
Tratamiento de datos personales de menores de edad y personas en estado de interdicción o incapacidad.
Cuarto. Cuando el responsable trate datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, como buena práctica, el aviso de privacidad integral podrá informar sobre tal situación, señalando al menos lo siguiente:
I. Los mecanismos que tiene implementados para recabar el consentimiento de la persona que ejerce la patria potestad, o en su caso, del tutor o representante legal, de conformidad con las reglas de representación dispuestas en el Código Civil Federal, y
II. Las acciones, medidas y previsiones especiales que caractericen este tipo de tratamiento y que lleve a cabo el responsable, a fin de salvaguardar el derecho a la protección de datos personales de estos grupos de personas.
Los Lineamientos fueron publicados en el Diario Oficial de la Federación del 17 de enero de 2013 y están disponibles en el vínculo electrónico <http://dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013

3.2. Los principios rectores que le dan contenido al derecho a la protección de datos personales

De acuerdo con la normatividad nacional, encontrando también su reflejo en los instrumentos, normas y estándares internacionales, el pilar central que sustenta el derecho fundamental a la protección de datos personales y que garantiza al individuo ese poder de decisión y control sobre la información que le concierne, se ha traducido en una serie de principios básicos de obligado cumplimiento y respeto para todos aquellos que utilizan datos personales en el desarrollo de sus actividades, los cuales son:

- Principio del consentimiento.
- Principio de información o transparencia.
- Principio de finalidad.
- Principio de proporcionalidad.
- Principio de calidad.
- Principio de licitud.
- Principio de lealtad.
- Principio de responsabilidad o rendición de cuentas.

Cabe mencionar que los anteriores principios fueron concebidos en una era predigital, por lo que actualmente existe una discusión internacional en torno a la eficacia de los mismos. Lo anterior lleva a reflexionar sobre la necesidad de crear nuevos marcos normativos multinacionales que puedan regular el flujo transfronterizo de datos a través de las fronteras, al tiempo que brinda seguridad a los internautas en un mundo multi-pantalla, sobre el debido tratamiento de sus datos.

Ahora bien, los principios de protección de datos se concretan en obligaciones[50] que les son exigibles a quien trata los datos personales, ya que tienen que hacerlo con apego a la normatividad aplicable para evitar así incumplimientos que se pueden traducir en una sanción o multa, sin perjuicio de la responsabilidad civil o penal que, en su caso, pudiera ser exigible.

[50] Para una comprensión de los principios en profundidad puede verse a Piñar Mañas y Ornelas Núñez, op. cit.

En concreto, conforme a la *Guía práctica para ejercer el derecho a la protección de datos personales*,[51] del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), se indican las obligaciones que tienen los particulares que usen datos personales, los responsables del tratamiento, y que son las siguientes:

Para la obtención y uso de tus datos personales, los particulares están obligados a:

- Darle un uso a los datos personales respetando la Ley, desde el momento de su obtención.

- No utilizar medios engañosos o fraudulentos para obtener los datos personales.

- Obtener tu consentimiento o autorización para el tratamiento de tus datos personales, salvo las excepciones previstas en el artículo 10 de la Ley.

- Darte a conocer el aviso de privacidad para que estés informado sobre quién y para qué recaba tus datos personales, cómo ejercer tus derechos ARCO, así como los términos y condiciones generales del tratamiento a los que será sometida tu información.

- Recabar sólo aquellos datos personales que sean necesarios para las finalidades para las que se obtienen.

Durante el tratamiento de tus datos personales:

- Sólo utilizar tus datos personales para las finalidades que autorizaste o consentiste.

- Mantener tus datos personales actualizados y correctos.

- Conservar tus datos personales sólo por el periodo que sea necesario para llevar a cabo la finalidad para la que se obtuvieron.

[51] Esta guía se encuentra disponible en el vínculo electrónico <http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf>,

- Sólo compartir tus datos personales con terceros si lo autorizaste, salvo las excepciones previstas en el artículo 37 de la Ley.

- Guardar la confidencialidad de tus datos personales.

- Implementar medidas de seguridad que eviten el daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de tus datos personales.

- Informarte si ha ocurrido una vulneración a la seguridad de las bases de datos que pueda afectar tus derechos patrimoniales o morales, para que puedas tomar las medidas que consideres necesarias en tu protección.

Una vez que ha concluido el uso de tus datos personales:

- Eliminar de las bases de datos o archivos tus datos personales, cuando hayan concluido las finalidades que dieron origen a su obtención.

Aunado a estas obligaciones existen los deberes de seguridad y confidencialidad.

La seguridad[52] consiste en que el responsable y, en su caso, el encargado del tratamiento, adopten medidas de seguridad administrativas, físicas y técnicas para proteger los datos personales contra su daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.[53]

Desde el punto de vista del uso de las TIC, los usuarios también deben

[52] Sobre la seguridad, véase a Lina Ornelas Núñez y Samantha Alcalde Urbina, "La seguridad como una pieza clave en el rompecabezas de la protección de datos personales", Retos de la protección de datos personales en el sector público, Instituto de Acceso a la Información Pública y Protección de Datos Personales en el Distrito Federal, diciembre de 2011. Disponible en el vínculo electrónico <http://www.infodf.org.mx/web/comsoc/campana/2012/LIbrodatosPweb.pdf>.

[53] En relación con las medidas de seguridad aplicables por responsables y encargados del tratamiento, véanse las "Recomendaciones en materia de seguridad de datos personales", publicadas en el Diario Oficial de la Federación del 30 de octubre de 2013 y disponible en el vínculo electrónico <http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013>.

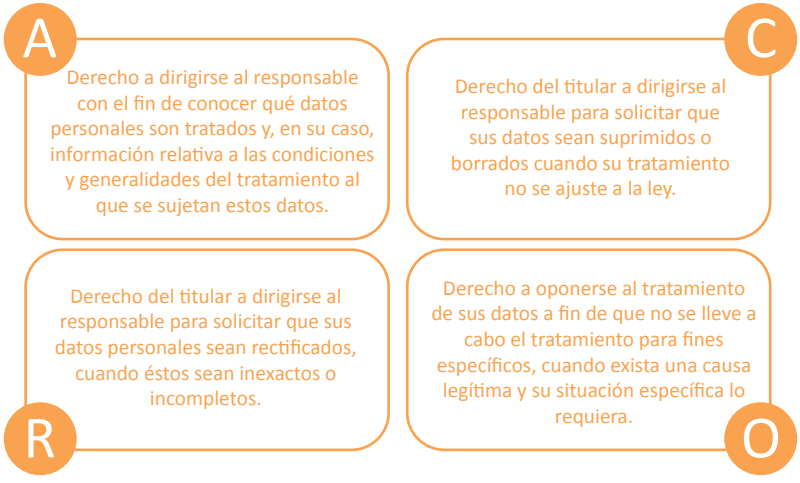
ser conscientes de la importancia de informarse acerca de los mecanismos de seguridad que ya están a disposición. Por tan sólo citar un ejemplo, cuando se efectúan compras en línea, los datos de la tarjeta de crédito se transmiten a través de una plataforma segura, lo que podemos identificar a través del "https" o el símbolo de un candado que vemos en la barra de dirección del navegador, lo que da lugar a que accedamos a un servidor seguro, basado en el uso de un certificado electrónico.

Y la confidencialidad consiste en que el responsable adopte medidas para garantizar que los datos personales que son tratados no sean revelados a terceros. Tanto el responsable como quienes intervengan en el tratamiento de los datos personales, deben guardar confidencialidad respecto de los datos personales a los que tengan acceso.

3.3. Los derechos inherentes a la protección de datos personales

El titular de los datos personales tiene reconocidos, en virtud de la Constitución y del desarrollo que realizó la LFPDPPP, los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO).

En cuanto al significado de cada uno de estos derechos, puede verse el siguiente gráfico:



En relación con estos derechos, su ejercicio requiere que el responsable adopte medidas para atender a los mismos[54] ya que el titular podrá ejercerlos en todo momento.

En el entorno electrónico se ha producido un intenso debate sobre el ya famoso "derecho al olvido", que incluso ha llegado a ser una de las razones por las que la Comisión Europea se plantease la reforma de la Directiva 95/46/CE.[55] En concreto, y al respecto, se cita el caso de un estudiante austríaco de Derecho que se dirigió a una red social de la que se había dado de baja para ver si todavía guardaban alguna información sobre él y se encontró con que mantenían 1 224 páginas con información suya, incluyendo fotografías, mensajes y posts relativos a varios años.

No obstante, el derecho al olvido es todavía un concepto, con importantes implicaciones tecnológicas[56] y también jurídicas. En cuanto a estas últimas, consideramos que el derecho al olvido debe ser entendido, en la práctica, como el derecho de cancelación y oposición, ya que no existe como tal. Y así lo ha puesto de manifiesto el Abogado General del Tribunal de Justicia de la Unión Europea en un caso que requiere de la interpretación de este último, por lo que se refiere a los buscadores de internet.[57]

54 Sobre el ejercicio de los derechos ARCO, véase la Guía práctica para la atención de las solicitudes de ejercicio de los Derechos ARCO, publicada por el IFAI y disponible en el vínculo electrónico <http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf>.

55 El 25 de enero de 2012, la Comisión Europea presentó una propuesta de reforma de la Directiva 95/46/CE en virtud de que ésta sería sustituida por un Reglamento General de Protección de Datos Personales. Con dicha reforma la Comisión Europea espera, entre otros objetivos, adecuar la norma europea general en materia de protección de datos personales a los avances tecnológicos que se han producido, ya que la citada Directiva fue publicada cuando todavía internet estaba en una fase incipiente, por lo que se refiere al uso comercial con el que lo conocemos.

56 Véase, al respecto, el estudio de ENISA titulado The right to be forgotten – between expectations and practice, del 20 de noviembre de 2012 y disponible, en inglés, en el vínculo electrónico <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport>.

57 Al respecto, véase las Conclusiones del Abogado General, Nilo Jääskinen, presentadas el 25 de junio de 2013 en el Asunto C-131/12, siendo las partes Google Spain, S.L., Google Inc vs. Agencia Española de Protección de Datos (AEPD) y M. C. G. En particular, sobre el derecho al olvido, el Abogado General indica que: "los artículos 12, letra b), y 14, letra a), de la Directiva, no establecen un derecho al olvido." Y también que: "propongo al Tribunal de Justicia que responda a la tercera cuestión en el sentido de que los derechos de supresión y cancelación de datos,

De igual forma, dado que ningún derecho es absoluto, debe tenerse en cuenta que si bien el titular de los datos puede manifestar su voluntad para que se elimine cierta información relativa a su persona, en ocasiones esto no sería posible, ya que pueden existir otros derechos en juego que deben sopesarse tales como la libertad de expresión, o la imposibilidad de borrar hechos históricos, entre otros temas.

Por tanto, los derechos ARCO, y en particular el que pudiera ser un futuro derecho al olvido, ponen de manifiesto la importancia de que el usuario de las TIC lea y se informe sobre a quién y para qué da sus datos personales, ya que consciente o inconscientemente, puede quedar "atrapado" en la red, incluso cuando intente cancelar su cuenta, debiendo considerar que desactivar no implica borrar. Es por ello que en el caso de los menores se requieren medidas específicas, ya que pueden no comprender ciertos términos o las consecuencias de sus acciones.

3.4. La protección de datos personales de menores en el uso de las tecnologías

Los menores son el centro de atención de los diferentes actores del ecosistema electrónico en lo que se refiere a la necesidad de medidas específicas de protección. Dicha protección es debida puesto que si bien se trata de "nativos digitales", pueden desconocer las implicaciones o consecuencias de sus acciones, además de que pueden ser el objetivo de acciones ilícitas por quienes hacen un uso también ilícito de las TIC.

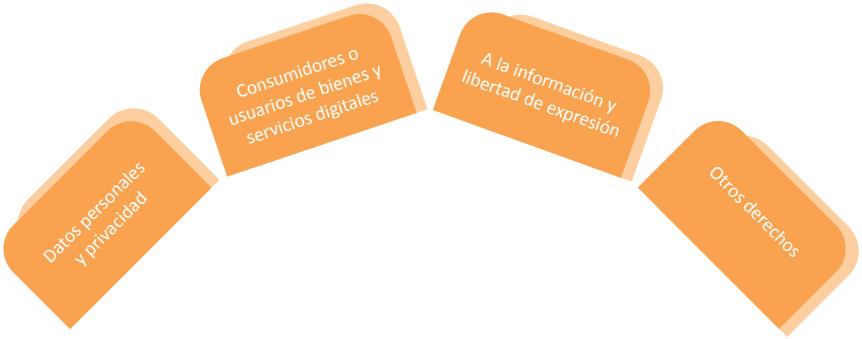
Debemos insistir en esto último, ya que las TIC *per se* no son malas, sino que hay quien hace un uso ilícito de las mismas para cometer diversas acciones delictivas.

Es por ello que tanto a nivel nacional como internacional los menores son el centro de atención de medidas, legislativas o de otra naturaleza,

establecidos en el artículo 12, letra b), y el derecho de oposición, recogido en el artículo 14, letra a) de la Directiva no se extienden a un derecho al olvido". Las Conclusiones del Abogado General pueden verse en el vínculo electrónico <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=795451>.

que tienen por objeto protegerles por lo que se refiere al uso, por los mismos o por terceros, de las TIC.

Dicha protección debe ser integral, en el sentido de que los menores son también titulares de derechos y, por lo tanto, las medidas que se adopten, cualquiera que sea su naturaleza, regulatoria o autorregulatoria, tienen que dar respuesta a las cuestiones que se plantean, entre las que se encuentran las siguientes:



En el ámbito internacional, son varios los instrumentos que tienen por objeto la protección de los menores, pudiendo citar al respecto, entre otros, la Convención sobre los Derechos del Niño,[58] que en su artículo 1 define al niño como "todo ser humano menor de 18 años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad". Además, es relevante tomar en consideración que dicha Convención indica en el apartado 1 de su artículo 3 que "en todas las medidas concernientes a las niñas y niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a la que se atenderá será el interés superior del niño".

[58] Adoptada y abierta a la firma y ratificación por la Asamblea General en su resolución 44/25, del 20 de noviembre de 1989 y que entró en vigor el 2 de septiembre de 1990, de conformidad con el artículo 49. El texto de la Convención está disponible en el vínculo electrónico <http://www2.ohchr.org/spanish/law/crc.htm>.

Otros instrumentos internacionales se centran en la necesidad de proteger a los menores frente a los diversos peligros a los que se exponen, y no sólo ellos porque los adultos también pueden ser víctimas de ciberdelitos o casos en los que vean vulnerados sus derechos como consumidores. En concreto, por lo que se refiere a la protección de los menores frente a contactos, conductas o contenidos inapropiados, es posible señalar aquí el Convenio de Lanzarote, adoptado por el Consejo de Europa;[59] y la Recomendación del Consejo de la OCDE relativa a la Protección de los Menores en Línea.[60] Estos instrumentos prevén, respectivamente, medidas para proteger a los menores contra la explotación y los abusos sexuales, así como dar recomendaciones para la elaboración de políticas de protección de los menores en línea.

Y a nivel nacional, este interés superior del niño se ha concretado en una reforma constitucional[61] en virtud de la que se reforman dos párrafos del artículo 4o., para elevar a rango constitucional el interés superior y derechos de la niñez,[62] y se reforma el artículo 73 de la Constitución para atribuir al Congreso facultades de manera que legisle en materia de derechos de niñas, niños y adolescentes.[63]

59 Se tratan de la Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS No. 201, abierto para su firma el 25 de octubre de 2007 y disponible, en inglés, en el vínculo electrónico <http://www.conventions.coe.int/Treaty/EN/treaties/Html/201.htm>.

60 Esta Recomendación, que fue adoptada el 16 de febrero de 2012, está disponible, en inglés, en el vínculo electrónico <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book>.

61 Decreto por el que se reforman los párrafos sexto y séptimo del artículo 4o. y se adiciona la fracción XXIX-P al artículo 73, de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación del 12 de octubre de 2011.

62 En concreto, los dos párrafos añadidos al artículo 4o. son los siguientes:
En todas las decisiones y actuaciones del Estado se velará y cumplirá con el principio del interés superior de la niñez, garantizando de manera plena sus derechos. Los niños y las niñas tienen derecho a la satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo integral. Este principio deberá guiar el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez.
Los ascendientes, tutores y custodios tienen la obligación de preservar y exigir el cumplimiento de estos derechos y principios.

63 Se adiciona la fracción XXIX-P en los términos siguientes:
XXIX-P. Expedir leyes que establezcan la concurrencia de la Federación, los Estados, el Distrito Federal y los Municipios, en el ámbito de sus respectivas competencias, en

3.5 Cinco premisas para lograr conciliar la exposición pública de los menores y adolescentes y su derecho a la privacidad

Se considera que las soluciones que se planteen a esta problemática deben partir de las siguientes premisas:

Primera: las niñas, niños y adolescentes nacieron en la Sociedad de la Información, son nativos y ciudadanos digitales. Un estudio[64] del Observatorio para la Seguridad de la Información, de marzo de 2009, da cuenta de una sustancial diferencia entre el uso que los adultos, las niñas, niños y los adolescentes dan a internet: mientras los primeros lo usan con una finalidad, es decir, "para algo", las niñas, niños y adolescentes reportan un uso más natural, lo utilizan para estudiar, charlar o escuchar música, de modo que constituye, para ellos, una herramienta básica de relación social e identidad.

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

Segunda: tener un enfoque positivo del tema dejando claro que el acceso a las redes sociales en internet es una increíble oportunidad para el ejercicio de los derechos (acceder a información, libertad de expresión, etc.) que, sin duda, contribuye al desarrollo integral de los menores y adolescentes en las dimensiones que propone la Convención de los Derechos del Niño: físico, social, material, espiritual y moral, así como otros instrumentos internacionales a los que nos hemos referido, pero sin perder de vista las amenazas existentes para sí o para terceros.

Tercera: asimismo, abordar el tema desde un enfoque fundamental-

materia de derechos de niñas, niños y adolescentes, velando en todo momento por el interés superior de los mismos y cumpliendo con los tratados internacionales de la materia, de los que México sea parte.

64 Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres, INTECO, 14 de marzo de 2009. Disponible en <http://www.inteco.es/file/O4-7X0FfwOb7HFjdHHpx7Q>.

mente preventivo y educativo, dejando claro la necesidad de erradicar ciertas prácticas intolerables que perjudican el desarrollo normal de los menores y adolescentes. Es decir, se trata de alcanzar un uso responsable y seguro, sin penalizar el uso de las TIC, ya que éstas no son nocivas o malas, sino el uso que se haga de las mismas. Por el contrario, las TIC aportan importantes beneficios a las personas, la sociedad en general, las empresas y las administraciones públicas.

Cuarta: diciendo "sí" a la tecnología y a los beneficios aparejados a ella, lo que refleja la necesidad de extender los aspectos posiTICvos de la Sociedad de la Información y el Conocimiento, así como aceptar que es necesario enfrentar las prácticas antisociales y perjudiciales para lograr el correcto desarrollo de las niñas, niños y adolescentes.

Quinta y última premisa: la responsabilidad compartida del Estado, la sociedad civil y la familia para abordar esta problemática, asegurando un protagonismo de la familia y el papel específico del propio Estado, incluyendo las autoridades educativas. De nuevo, fomentar el uso seguro y responsable de las TIC.

4. MARCOS NORMATIVOS, INICIATIVAS DE COOPERACIÓN Y ACTORES FUNDAMENTALES PARA LA PROTECCIÓN DE MENORES EN LA ERA DIGITAL

Este capítulo aborda los marcos normativos nacionales e internacionales que existen para proteger distintos aspectos relacionados con los menores, con especial énfasis en aquellos relativos a sus actividades en línea. Asimismo, se abordan aspectos de cooperación internacional, así como la necesidad de legislar tomando en cuenta las mejores prácticas en la materia. Se mapean los actores interesados que necesariamente deben involucrarse en el desarrollo de una política pública, así como el abordaje educativo como el eje rector de la misma.

4.1 Marcos normativos e iniciativas no vinculantes

Entre las reformas constitucionales que se han aprobado en México en los últimos años, cabe destacar la publicada en el *Diario Oficial de la Federación* del 12 de octubre de 2011, por la que se reforman los párrafos sexto y séptimo del artículo 4 y se adiciona la fracción XXIX-P al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos.

Dicha reforma es relevante en materia de protección de los menores, ya que se consiguen dos importantes objetivos. Por un lado, se eleva a rango constitucional el interés superior y los derechos de la niñez; por otro, se faculta al Congreso para legislar en materia de niñas, niños y adolescentes.

Mientras que en México se consagraba constitucionalmente el principio del "interés superior de la niñez", que debe guiar y ser el objetivo de toda política pública relacionada con los menores de edad, a nivel mundial se producían importantes avances en foros internacionales a través de la adopción de medidas que tienen como destinatarios a los menores.

Es así que, a modo de ejemplo, en el ámbito de la Unión Europea, se publicaba la Directiva 2011/93/UE[65] del Parlamento Europeo y del Consejo del 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil, y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo; la Organización para la Cooperación y el Desarrollo Económico (OCDE) promulgaba, el 16 de febrero de 2012, una Recomendación del Consejo de la OCDE sobre la Protección de los Menores en Línea (*Recommendation of the Council on the Protection on Children Online*); y más recientemente, el año pasado, la International Centre for Missing & Exploited Children publicaba en el mes de enero un Modelo de Ley de Protección de Niños.

Un ejemplo muy concreto de medidas que pueden adoptarse por parte de la industria para proteger a los menores en línea es el de la Unión Internacional de Telecomunicaciones (International Telecommunications Union, ITU) y UNICEF a través de la publicación de una Guía para la Industria sobre la Protección de los Menores en Línea *(Guidelines for Industry on Child Online Protection)*.[66]

Pero mientras que en los diferentes foros internacionales se avanza de manera incesante para proteger a los menores en línea, quizás México se ha quedado rezagado, siendo necesario que se adopten medidas específicas, legislativas o no, e incluso una combinación de ambas, para impulsar la protección de los menores mexicanos. No hacer nada no es una opción en este caso y ahora le toca a México cumplir con sus compromisos internacionales. Al mismo tiempo, México tiene la oportunidad de aportar soluciones efectivas que puedan servir de guía a otros países.

[65] El número de la Directiva es 2011/93/UE y no 2011/92/UE, según la corrección de errores publicada en el Diario Oficial de la Unión Europea L, núm. 18, del 21 de enero de 2012.

[66] Pueden consultarse en <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-COP.IND-2013-PDF-E.pdf>.

Sin perjuicio de normas marco para la protección de los menores, tales como la Convención de las Naciones Unidas sobre los Derechos del Niño,[67] en cuanto a la normatividad y otros instrumentos, legislativos o no, deben tomarse en consideración los que se indican en la siguiente tabla, dado que pueden ser una guía para el legislador nacional.

[67] Adoptada y abierta a la firma y ratificación por la Asamblea General en su resolución 44/25, del 20 de noviembre de 1989, que entró en vigor el 2 de septiembre de 1990 y que está disponible, en español, en la dirección electrónica <http://www2.ohchr.org/spanish/law/crc.htm>.

Organización internacional o supranacional	Acrónimo	Instrumento	Fecha	Fuente
Organización para la Cooperación y el Desarrollo Económico	OCDE	Declaración de Seúl sobre el Futuro de la Economía de Internet (*The Seoul Declaration for the Future of the Internet Economy*).	18/6/2008	http://www.oecd.org/sti/ieconomy/40839436.pdf
		Recomendación del Consejo de la OCDE sobre la Protección de los Menores en Línea (*Recommendation of the Council on the Protection on Children Online*).	16/2/2012	http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book=
Consejo de Europa	COE	Convenio (201) del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual.	25/10/2007	http://www.coe.int/t/dghl/standardsetting/children/Source/LanzaroteConvention_es.pdf
		Convenio (185) del Consejo de Europa sobre el Cibercrimen.	23/11/2001	http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_spanish.PDF
Unión Europea	UE	Directiva 2010/13/UE del Parlamento Europeo y del Consejo, del 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual).[68]	10/3/2010	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:095:0001:0024:ES:PDF

[68] La Directiva 2010/13/UE, publicada en el Diario Oficial de la Unión Europea L, número 95, del 15 de abril, derogó parcialmente a la Directiva 2007/65/CE del Parlamento Europeo y del Consejo, del 11 de diciembre de 2007, por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, publicada en el Diario Oficial de la Unión Europea L, número 332, del 18 diciembre, disponible en español en la dirección de internet <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:332:0027:0045:ES:PDF>.

Organización internacional o supranacional	Acrónimo	Instrumento	Fecha	Fuente
Unión Europea	UE	Directiva 2011/93/UE del Parlamento Europeo y del Consejo, del 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil, y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.	13/12/2011	http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:ES:PDF
International Centre for Missing & Exploited Children	ICMEC	Modelo de ley de protección de niños.	Enero de 2013	http://www.icmec.org/en_X1/icmec_publications/CP_Model_Law_Final_January_2013_Spanish.pdf
Otras	IIJusticia	Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes (Memorandum de Montevideo).	28 /07/2009	http://www.iijusticia.org/docs/MemoMVD_Es.pdf

Por su relevancia y transcendencia, se destacan los Convenios del Consejo de Europa. Su importancia se debe a que el Consejo de Europa cuenta con diversos Convenios que deben ser tomados en consideración a la hora de elaborar una estrategia, ya que se refieren a materias tales como el cibercrimen, la protección de datos personales, la transparencia u otras. Además, sería conveniente que México considerara su firma y ratificación, con las respectivas reservas y declaraciones que, en su caso, estime oportunas.

— Convenio para la protección de los niños contra la explotación y el abuso sexual

Pese a que México es uno de los Estados no miembros del Consejo de Europa, puede firmarlo y ratificarlo, si bien hasta la fecha no lo ha hecho.[69]

Este Convenio entró en vigor el 1 de julio de 2010, al haberse cumplido la condición de que fuera ratificado por cinco países, de los que al menos tres fueran Estados miembros del Consejo de Europa. Además, el Convenio cuenta con un informe explicativo.[70]

— Convenio sobre el Cibercrimen

Al igual que en el caso del Convenio para la protección de los niños contra la explotación y el abuso sexual, México no ha firmado ni ratificado dicho Convenio.

El Convenio entró en vigor el 1 de julio de 2004, al haber sido ratificado por cinco países, de los que al menos tres fueran Estados miembros del Consejo de Europa.[71]

69 La lista de países, ya sean Estados miembros o no del Consejo de Europa, que han firmado o ratificado el citado Convenio, actualizada y consultada en diciembre de 2013, puede consultarse en <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=&CL=ENG>.

70 Disponible, en inglés, en <http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm>.

71 La lista de países que han firmado o ratificado el Convenio se encuentra disponible y actualizada, en la dirección de internet <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

Dicho Convenio cuenta también con un informe explicativo.[72]

En cuanto a los instrumentos, normativos o de otra naturaleza, indicados anteriormente, es necesario tomar en consideración que además de tener una diferente naturaleza, abordan la cuestión de la protección de los menores en línea desde diferentes puntos de vista, los cuales serían complementarios, si bien actualmente no hay un instrumento específico a nivel internacional que vincule a todos los países, lo que hace que surjan diferencias a la hora de proteger a los menores.

La siguiente tabla tiene por objeto poner de manifiesto algunas de estas diferencias, las cuales deben tomarse en consideración a la hora de adoptar medidas en el caso de México:

[72] Disponible, en inglés, en <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Organización internacional o supranacional	Norma/Instrumento	Carácter legislativo	Vinculante para países o Estados miembros	Previsión de protección integral de los menores online (protección de datos personales, delitos, etc.)	Cooperación internacional
Organización para la Cooperación y el Desarrollo Económico (OCDE)	Declaración de Seúl sobre el Futuro de la Economía de Internet (*The Seoul Declaration for the Future of the Internet Economy*).	No	No	No se trata de una Declaración referida a la economía digital en la que únicamente se hace referencia a la necesidad de protección de los menores en línea. Por tanto, no es un instrumento que tenga por objeto la protección de los menores en línea como tal.	No específicamente en materia de protección de los menores en línea.
	Recomendación del Consejo de la OCDE sobre la Protección de los Menores en Línea (*Recommendation of the Council on the Protection on Children Online*).	No	No	Es un instrumento relativo a la protección de los menores en línea, si bien se limita a una serie de principios y recomendaciones a las partes interesadas (*stakeholders*) en cuanto a la protección de los menores en línea. Su ámbito es limitado, ya que excluye expresamente las cuestiones relativas a pornografía infantil y abusos sexuales al indicar que son objeto de otros instrumentos internacionales. Es decir, no trata cuestiones relativas a riesgos relacionados con imágenes de abusos o explotación sexual, ya que se remite en este punto a otros instrumentos internacionales.	No prevé mecanismos específicos de cooperación internacional, ya que se trata de recomendaciones.
Consejo de Europa (CoE)	Convenio (201) del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual.	No	Sólo tras su firma y ratificación	El Convenio se centra específicamente en la protección de los menores contra su explotación y el abuso sexual, tratando cuestiones relativas a la pornografía infantil, pero sin abordar otros aspectos relativos a su protección en línea, tales como sus datos personales o la protección contra acciones de marketing abusivo.	Entre sus objetivos está el de promover la cooperación internacional para mejorar la lucha contra la explotación y el abuso infantil, si bien se remite a la cooperación mediante instrumentos internacionales y regionales aplicables.

Organización internacional o supranacional	Norma/Instrumento	Carácter legislativo	Vinculante para países o Estados miembros	Previsión de protección integral de los menores online (protección de datos personales, delitos, etc.)	Cooperación internacional
Consejo de Europa (CoE)	Convenio (185) del Consejo de Europa sobre el Cibercrimen.	No	Sólo tras su firma y ratificación	Entre los delitos que trata, incluye el de pornografía infantil, pero no aborda otras cuestiones o asuntos sustantivos relativos a la protección de los menores en línea.	Incluye disposiciones sobre la asistencia mutua en materia de investigaciones o procedimientos relativos a solicitudes de asistencia mutua en caso de que no haya acuerdos internacionales aplicables.
Unión Europea	Directiva 2010/13/UE del Parlamento Europeo y del Consejo, del 10 de marzo de 2010, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual).	Sí	Sí, para los Estados miembros de la Unión Europea	Se centra en contenidos audiovisuales que puedan ser dañinos u ofensivos para los menores. En particular, pone énfasis en la protección de los menores en la radiodifusión televisiva.	Prevé la cooperación entre organismos reguladores, si bien se limita al objeto de la citada Directiva, de manera que no se refiere a otras autoridades competentes, cualquiera que sea su naturaleza.

Organización internacional o supranacional	Norma/Instrumento	Carácter legislativo	Vinculante para países o Estados miembros	Previsión de protección integral de los menores online (protección de datos personales, delitos, etc.)	Cooperación internacional
Unión Europea	Directiva 2011/93/UE del Parlamento Europeo y del Consejo, del 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales, la explotación sexual de los menores y la pornografía infantil, y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo.	Sí	Sí, para los Estados miembros de la Unión Europea	Se centra específicamente en los delitos contra menores, tanto pornografía infantil como abusos sexuales. Lo anterior supone que otras cuestiones relativas a la protección de los menores no sean objeto de esta Directiva, debiendo recurrir, en su caso, a otras normas de la Unión Europea.	Promueve la cooperación en las cuestiones que trata por los Estados miembros con otros países. Al respecto, se remite a que los Estados miembros hagan uso de tratados bilaterales o multilaterales.
International Centre for Missing & Exploited Children	Modelo de ley de protección de niños.	No	No	Limita el abuso a padres, tutores o personas a cargo del cuidado del niño u otra persona que tenga una posición de confianza o autoridad (art. 2.2). Además, aunque hace referencia a internet, no está pensado específicamente para el entorno electrónico. Tampoco hace referencia a materiales específicos, como la protección de datos personales o los riesgos a los que pueda estar expuesto el menor en su consideración como consumidor.	Prevé la necesidad de cooperación internacional, tanto por lo que se refiere al intercambio de información sobre mejores prácticas como en la lucha contra actos delictivos.

Organización internacional o supranacional	Norma/Instrumento	Carácter legislativo	Vinculante para países o Estados miembros	Previsión de protección integral de los menores online (protección de datos personales, delitos, etc.)	Cooperación internacional
IIJusticia	Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes (Memorandum de Montevideo). *	No	No	A pesar de que trata una amplia variedad de temas, tales como protección de datos personales, pornografía infantil, etc., se limita a proporcionar recomendaciones dirigidas a varias partes interesadas (stakeholders) a modo de política pública y con un enfoque que se centra específicamente en la protección de datos personales en redes sociales en internet.	Promueve la cooperación a nivel internacional por las diferentes partes interesadas.

Fuente: Elaboración propia.

* Puede consultarse en <http://iijusticia.org/Memo.htm>.

A la vista de cada uno de estos instrumentos internacionales, la adopción de medidas específicas en el caso de México debería partir de una combinación de las previstas en aquéllos, puesto que, además de tener una diferente naturaleza, legislativa o no y vinculante o no, se centran en cada caso en aspectos o cuestiones que pueden diferir en cuanto al alcance.

Por último, la protección de los menores en línea requiere de una aproximación activa por las partes interesadas, en el sentido de que no se trata de adoptar medidas en un momento determinado sobre una cuestión específica, sino de acciones constantes que permitan garantizar una protección efectiva de manera que los menores y el resto de usuarios se puedan beneficiar del uso de las TIC, tanto como usuarios de bienes o servicios ofrecidos a través de medios electrónicos o basados en los mismos, así como en su condición de ciudadanos digitales.

4.2 Otros referentes internacionales

Son varios los referentes que se encuentran a nivel internacional y que se concretan, fundamentalmente, en informes específicos en materia de protección de menores en línea que han sido publicados en diferentes foros internacionales. No está dentro de los alcances del presente ensayo plasmar las excelentes recomendaciones derivadas de los mismos, sino tan sólo describir en términos generales sus objetivos, así como aportar las ligas donde se encuentra mayor información al respecto.

Puesto que se trata de instrumentos que sirven de base para la toma de decisiones a la hora de desarrollar, implementar o evaluar una política pública, e incluso respecto de los que cabría considerar la participación, directa o indirecta, en los mismos, a continuación se listan los mismos:

REFERENTES INTERNACIONALES SOBRE PROTECCIÓN DE MENORES EN LÍNEA

Unión Internacional de Telecomunicaciones (UIT)	Directrices sobre Protección de la Infancia en Línea para los encargados de formular políticas (2009)	— Proporciona directrices dirigidas a los encargados de formular políticas públicas con un claro enfoque jurídico. — Presta atención a los riesgos, especialmente a los derivados de contenidos pedófilos. — Incluye lista de actividades nacionales y partes interesadas.
Organización para la Cooperación y el Desarrollo Económico (OCDE)	Report on risks faced by children online and policies to protect them (2012)	— Incluye una tipología de riesgos, excluyendo aquéllos a los que se refieren los Convenios del Consejo de Europa, así como los riesgos generados por niños para otros niños. — Presenta algunas opciones de política pública a la vista de experiencias de diferentes países.
International Centre for Missing & Exploited Children (ICMEC)	Pornografía infantil: Modelo de Legislación y Revisión Global (2012)	— Hace referencia a algunos aspectos que deben tomarse en consideración al elaborar una ley en la materia. — Incluye una comparativa internacional, no exhaustiva, de legislaciones que tipifican delitos y responsabilidad de prestadores de servicios de información.
UNICEF	Child Safety Online: Global challenges and strategies, Technical report (Mayo de 2012)	— Trata la cuestión desde el punto de vista de los riesgos y las medidas de protección, tanto online como offline. — Principalmente se refiere a contenidos. — Incluye cuatro objetivos clave para una política pública, siendo el menor el centro de la misma.
UIT y UNICEF	Draft Guidelines for Industry on Child Online Protection (Diciembre de 2013)	— Se dirigen a prestadores de servicios, con la finalidad de garantizar un internet más seguro. — Incluyen un amplio rango de medidas con diferentes opciones de política pública, así como una lista de comprobación (checklist) para sectores específicos.

En el caso de la Guía para la Industria sobre Protección de los Menores en Línea *(Guidelines for Industry on Child Online Protection)*, se trata de la actualización de la Guía ya publicada,[73] que se adoptó hace cuatro años.

Cabe señalar que, excepto en el caso de la Guía citada y de las Directrices de la UIT sobre Protección de la Infancia en Línea para los encargados de formular políticas, el resto de referentes internacionales son informes que tienen por objeto comparar las acciones adoptadas por diversos ordenamientos jurídicos alrededor del mundo.

Además de los referentes indicados, en el caso de la UIT proporciona varios listados de recursos a nivel internacional relativos específicamente a la industria,[74] educadores[75] y menores.[76]

En el caso de la industria, existe un firme compromiso por aportar consejos, guías prácticas e información relevante a los usuarios por parte de grandes empresas como Microsoft y Google, entre otras. Una muestra de ello, es la guía *Está bien saberlo: una guía para mantenerse seguro y protegido en internet*,[77] que en sus contenidos se refiere específicamente a la seguridad de la familia en internet. Asimismo, el portal Navega protegido aporta información clara sobre el uso seguro y responsable de la tecnología.[78]

---

73 De 2009 y disponible en <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/industry/industry.pdf>.

74 Véase <http://www.itu.int/osg/csd/cybersecurity/gca/cop/industry.html>.

75 Véase <http://www.itu.int/osg/csd/cybersecurity/gca/cop/educators.html>.

76 Véase <http://www.itu.int/osg/csd/cybersecurity/gca/cop/children.html>.

77 Disponible en la dirección de internet <http://www.google.com.mx/goodtoknow>. Para Google, existe cero tolerancia en torno al abuso sexual infantil. El buscador impide que pueda accederse a páginas con pornografía infantil y ha desarrollado una semántica especializada para lograrlo, así se intente bajo innumerables posibilidades y denominaciones. Asimismo, equipos de ingenieros trabajan día a día para desarrollar mecanismos tecnológicos para detectar imágenes en videos que involucren menores abusados. De igual forma, su departamento legal facilita investigaciones y da aviso a las autoridades correspondientes cuando se detectan casos concretos. A partir de tecnología desarrollada por Microsoft, se pueden identificar, asimismo, imágenes de fotografías de menores en riesgo que luego se pueden bajar de manera automática mediante el mecanismo "hash" de identificación. Éste es un claro ejemplo de cooperación entre la industria en el mejor interés de los menores.

78 <www.navegaprotegido.org>.

4.3 Reformas legislativas en México

Si bien a finales de 2013 se han presentado varias iniciativas legislativas en el Congreso, entre las que destacan dos que se refieren, respectivamente, al uso seguro de internet y la reforma del Código Penal Federal para luchar contra el "cybergrooming" o "cortejo",[79] ninguna de éstas afrontan todos los aspectos que se deben considerar en una política pública efectiva en materia de protección de los menores en línea.

Queremos resaltar la importancia de que cualquier marco normativo que los legisladores quieran crear o modificar, en la búsqueda de brindar mayor protección a los menores, debe tomar en cuenta todos los derechos en juego. En particular, el diseño de tipos penales específicos debieran considerar la conducta y no penalizar el medio (internet).

En ese sentido, tan sólo por citar un ejemplo, abordaremos aspectos generales de la iniciativa que reforma los artículos 7 de la Ley Federal de Telecomunicaciones y 36 de la Ley Orgánica de la Administración Pública Federal,

[79] Se trata de la iniciativa que adiciona el artículo 259 Ter al Código Penal Federal para tipificar una serie de conductas haciendo uso de las nuevas tecnologías de la información que atentan contra la identidad sexual de las niñas, niños y adolescentes, de la diputada Martha Leticia Sosa Govea (PAN). Turnada a la Comisión de Justicia 3873'IV. GP1 núm. 3873'IV, del 1/10/2013.
Asimismo, se citan las siguientes iniciativas:
Televisión; y para la Protección de los Derechos de Niñas, Niños y Adolescentes. Presentada por la diputada Lucila Garfias Gutiérrez, Nueva Alianza. Turnada a las Comisiones Unidas de Salud, de Radio y Televisión y de Derechos de la Niñez. Gaceta Parlamentaria, número 3853-III, jueves 5 de septiembre de 2013. (1260)
— Que reforma y adiciona diversas disposiciones del Código Penal Federal, en materia de protección de los derechos de niñas, niños y adolescentes. Presentada por la diputada Martha Leticia Sosa Govea, PAN. Turnada a la Comisión de Justicia. Gaceta Parlamentaria, número 3873-IV, martes 1 de octubre de 2013. (1568)
— Que reforma el capítulo quinto y el artículo 21 de la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, con el fin de garantizarles el acceso a una vida libre de violencia. Presentada por la diputada Rocío Adriana Abreu Artiñano, PRI. Turnada a la Comisión de Derechos de la Niñez. Gaceta Parlamentaria, número 3885-VIII, martes 15 de octubre de 2013. (1573)
— Que reforma los artículos 1o. y 3o. de la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, para establecer la aplicación de los tratados internacionales y los principios en materia de derechos humanos, encaminados a la protección y prevención del maltrato infantil, así como para asegurar su normal desarrollo psicosexual. Presentada por la diputada María Fernanda Schroeder Verdugo, PRI. Turnada a la Comisión de Derechos de la Niñez. Gaceta Parlamentaria, número 3892-VI, jueves 24 de octubre de 2013. (1622)

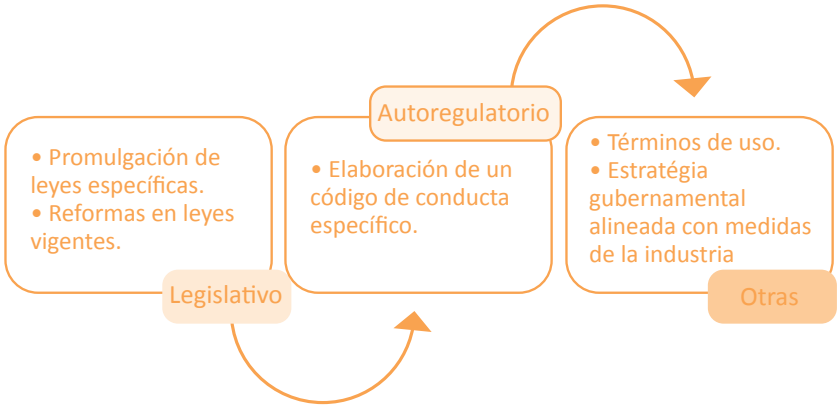
en materia de acceso seguro a internet por parte de niñas, niños y jóvenes.[80] La iniciativa tiene por objeto que la Secretaría de Comunicaciones y Transportes (SCT) pueda expedir las normas oficiales mexicanas en materia de telecomunicaciones y aquellas relacionadas con el acceso seguro a internet por parte de niñas, niños y adolescentes. Asimismo, otorga facultades a la SCT para establecer normas oficiales que contengan especificaciones y requerimientos para la instalación y operación del servicio de internet seguro destinado a menores en espacios públicos.

Cabe mencionar que dicha iniciativa, tal como está planteada, puede suponer y tener un efecto negativo, ya que se basaría en el filtrado de contenidos que sería contrario a la libertad de expresión. Otros efectos negativos serían, paradójicamente, el tratamiento de datos personales de menores, la imposibilidad de acceder a contenidos que pese a ser lícitos hayan sido clasificados como ilícitos, y la posibilidad de adoptar una postura excesivamente proteccionista, incluso creando desigualdades en caso de que haya diferentes estándares en cuanto a los contenidos. Por otra parte, el establecimiento de normas oficiales, si no se hace de manera adecuada, puede conllevar una limitación a la innovación y al desarrollo de las TIC en México.

En definitiva, es importante que se tomen en cuenta a la hora de legislar las mejores prácticas internacionales en la materia y se abran foros abiertos al debate, en donde todas las voces sean escuchadas, incluidos los menores.

Por lo anterior, proponemos un enfoque holístico de medidas, en el que es necesario contar con disposiciones legales obligatorias, pero también con otro tipo de acciones como las siguientes.

[80] Presentada por el Dip. Fernando Alejandro Larrazábal Bretón (PAN). Turnada a las Comisiones Unidas de Comunicaciones y de Gobernación, GP núm. 3853-III, 5/9/2013. La iniciativa señala alguna información relevante, como por ejemplo que la actividad de monitoreo de internet por parte de la Policía Federal Preventiva ha dado como resultado encontrar 1 347 sitios que exhiben pornografía infantil, de los cuales 310 son mexicanos.



Fuente: Elaboración propia.

4.4 Cooperación internacional

Respecto a la cooperación internacional, ésta es necesaria en todos los niveles en los que se pueda desarrollar la política pública, comenzando con la cooperación entre los sectores público y privado, siguiendo a nivel regional y continuando a nivel internacional (dado el carácter transnacional del internet y la computación ubicua).

Entre los instrumentos adecuados para garantizar dicha cooperación pueden encontrarse desde los informales, tales como la participación en foros internacionales, hasta formales, como los Tratados de Asistencia Legal Mutua (en inglés, Mutual Legal Assistance Treaties, MLTAs).

En relación con estos tratados de asistencia mutua, el Convenio sobre el Cibercrimen antes citado puede ser una buena muestra, ya que prevé la asistencia mutua como una medida de luchar contra los ciberdelitos.[81]

[81] Al respecto, los dos primeros párrafos del artículo 25 del Convenio, indican lo siguiente:

La cooperación debe permitir alcanzar, entre otros objetivos, los siguientes:

- Una interrelación e interactuación que permita el intercambio de información y buenas prácticas;

- Alcanzar un alto nivel de protección de los menores en línea; y

- Cooperar en interés de los menores sin que ello suponga un obstáculo al desarrollo tecnológico.

4.5 Actores fundamentales

Una política pública para la protección de menores en línea debe tomar en cuenta a todos los actores interesados:

- Los propios menores de edad.
- Padres o tutores.
- Autoridades/gobierno:
  - Educativas.
  - De procuración e impartición de justicia (en los ámbitos federal y local).
  - Policías cibernéticas (federal y locales).
  - Legisladores.
- Industria.
- Sociedad civil.

Lo anterior bajo un marco de cooperación internacional.

Artículo 25. Principios generales relativos a la asistencia mutua.
1. Las partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.
2. Cada parte adoptará, asimismo, las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

4.6 La educación y prevención como abordaje fundamental

El abordaje educativo debe vislumbrarse estrictamente como el necesario empoderamiento de los usuarios para prevenir riesgos y aprovechar al máximo las ventajas de la sociedad de la información. Este abordaje está dirigido a todas las personas pero fundamentalmente a los menores y adolescentes, y de preferencia en la enseñanza regular.

De esta manera, a las niñas, niños y adolescentes se les debe inculcar la comprensión del espíritu de protección de la vida privada de ellos y de los demás, en el uso responsable y seguro de internet y las redes sociales digitales, para que vean a internet como un espacio con normas y que las acciones allí realizadas tienen consecuencias, en particular deben conocer:

- Que la distribución de pornografía, el acoso, la discriminación, la promoción del odio racial, la difamación y la violencia son ilegales y penados por la ley.

- Sobre el respeto de la vida privada, buen nombre e intimidad de terceras personas.

- Las posibles responsabilidades civiles, penales o administrativas derivadas del uso abusivo de internet.

Asimismo, se debe educar a las niñas, niños y adolescentes sobre las políticas de privacidad, seguridad y de alertas de las distintas redes sociales, y de la "incertidumbre" que rodea a la veracidad de la información publicada en internet, a efecto de que ellos mismos discriminen las fuentes.

Por otro lado, se debe recalcar a los menores y adolescentes que el uso de pseudónimos es aceptado, siempre que éstos no sirvan para engañar o confundir respecto a la identidad de una persona, haciendo énfasis en los riesgos de ser engañados sobre la identidad de la otra persona y los robos o la suplantación de identidad.

Otro punto importante es que el proceso de promoción y educación sobre la sociedad de la información, así como el uso responsable y seguro de internet y las redes sociales, debe ser permanente. Para ello debe incluirse en los planes educativos de todos los niveles y considerarse la participación de todos los actores involucrados en el diseño de los materiales, siempre tomando en cuenta las particularidades culturales y locales de los menores y adolescentes.

Los docentes también deben ser formados en estos temas. Las autoridades educativas -con el apoyo de las autoridades de protección de datos personales, organizaciones de la sociedad civil y académicos- debemos asistirlos y brindarles todo el acompañamiento y apoyo técnico necesarios. En este sentido, existen ya recomendaciones concretas para facilitar la tarea de los educadores como guías, dado que muchas veces son migrantes digitales y no logran transmitir con facilidad y sin miedos o atavismos, los mensajes adecuados a los chicos.[82]

Asimismo, deben crearse mecanismos o plataformas en los propios centros educativos donde las niñas, niños y adolescentes tengan la posibilidad de resolver los conflictos derivados del uso de internet y las redes sociales, sin prejuicios y bajo la más estricta confidencialidad que el problema lo requiera.

Para mayor información se adjuntan las recomendaciones del Memorandum de Montevideo que prevé recomendaciones específicas para que las autoridades educativas aborden la problemática objeto de este documento.

[82] Ver Anexo I del Memdorandum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes, disponible en <http://iijusticia.org/Memo.htm>.

CONCLUSIONES A MANERA DE REFLEXIÓN

Ha quedado claro que los nativos digitales merecen contar con una protección comprehensiva que surja de la prevención y la educación. A partir de estos ejes, es necesario que toda solución emane de las siguientes premisas:

- Las niñas, niños y adolescentes son titulares de todos los derechos humanos de que gozan los mayores.

- La obligación que tenemos los mayores de tomar en cuenta las opiniones de los niñas, niños y adolescentes en función de su edad y madurez.

- El derecho a una protección especial en aquellas situaciones que resulten perjudiciales para sus derechos, en particular su desarrollo integral.

- El reconocimiento del principio del interés superior del menor, no como cláusula que

permita la discrecionalidad adulta para la restricción de los derechos, sino como una fórmula precisa que obliga a promover su respeto y garantía en un marco de estricta ponderación de los beneficios que las medidas se tomen, especialmente aquellas de carácter restrictivo.

- La responsabilidad es cien por ciento compartida, incluyendo a la familia y demás actores como el Estado, autoridades administrativas, legislativas y judiciales, sociedad civil organizada, industria y sociedad en general.

- Internet no puede ser pensado como un esquema técnico de transmisión de información, sino como un sistema complejo articulado con todas las instancias socioeconómicas determinantes de las formas de socialización. Estudiando la red de relaciones de los menores y jóvenes internautas, vemos que internet, significa un importante espacio de socialización que desencadena relaciones de proyección, identificación e intersubjetividad, participando activamente en la producción de una imagen de sí mismo y de la construcción de la identidad, potencializando la capacidad de comunicación, acceso y distribución de información sobre el mismo y sobre sus pares de una manera nunca antes posible.

- Los educadores necesitan adecuarse, no apenas a los equipamientos en las escuelas, sino también comprender la dinámica de interacción que las nuevas generaciones de alumnos establecen con la información y con las instituciones sociales.

Las TIC están al servicio de las personas, ya sean éstas menores o adultas, y permiten interrelaciones así como el acceso y la gestión de información en un modo revolucionario. Lo anterior implica que en el ecosistema digital todos tengamos un papel y seamos responsables de nuestras acciones, de manera que debemos hacer un uso seguro y responsable de las mismas sin perjuicio de la protección que nos confieren las diferentes autoridades competentes, así como los esfuerzos de la industria por mantener un entorno seguro que nos permita una experiencia positiva.

Por último, consideramos que los elementos que deben considerarse para crear una política pública integral en esta materia serían los siguientes:

— Referentes internacionales para una política pública sobre protección de los menores en línea. El desarrollo de un instrumento a nivel nacional para proteger a los menores en línea no parte de cero, sino que cuenta con varios referentes, tanto legislativos como de otra naturaleza, a nivel internacional. Es así que el planteamiento de una política pública en esta materia debería tomar en consideración los instrumentos normativos y los modelos de leyes que se han desarrollado en diversos foros y por diferentes organizaciones internacionales. Dichos instrumentos son referentes para otros países, si bien la ausencia de indicadores específicos hacen que resulte complejo identificar modelos nacionales a seguir.

— Tomar en consideración principios fundamentales en el diseño. El instrumento que se desarrolle en México debe partir del principio relativo al interés superior de la niñez y debe basarse en los principios relativos a la responsabilidad compartida de las partes involucradas en la adopción de medidas, la neutralidad tecnológica de manera que no se centre únicamente en una tecnología específica, respetar los derechos de los menores y de otros usuarios de las TIC (libertad de expresión, protección de datos y privacidad, así como libertad de recibir información). También, las medidas que se adopten deben ser proporcionales a los riesgos que se quieren evitar. Por tanto, son principios que deben estar presentes en el diseño del instrumento que se adopte y de las acciones que se lleven a cabo.

— Promover objetivos fundamentales. En virtud de la política pública de protección de los menores en línea, se deben promover objetivos fundamentales comenzando con el hecho de reconocer a los menores como titulares de derechos que permitirán asegurar su desarrollo como ciudadanos digitales y también como usuarios de las TIC. Unido a lo anterior, se debe promover también la responsabilidad compartida tanto del sector público como privado, el uso seguro y responsable de las TIC, así como la cooperación internacional en esta materia.

En el desarrollo de una política pública sobre protección de los menores en línea se debe partir de los referentes internacionales, normativos y de otra naturaleza, ya existentes, prestando atención a las buenas prácticas que permitan maximizar los principios fundamentales que han de estar presentes en el diseño de instrumentos y medidas, así como promover objetivos fundamentales.

Los desafíos son grandes, pero las voluntades también. Cada actor, desde su ámbito de competencia, debe aportar elementos que faciliten una protección efectiva de nuestros menores en la era digital. Este ensayo es tan sólo un punto de partida para iniciar esa conversación.

ANEXO 1

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 de internet y las redes sociales digitales, fundamentalmente por medio de la educación, considerando la participación activa de los propios niños, niñas y adolescentes, los progenitores u otras perso-

nas a cargo de su cuidado y los educadores, tomando en consideración como principio fundamental el interés superior de niñas, niños y adolescentes.

Para esto se debe tomar en consideración las siguientes recomendaciones:

1. Los Estados y las entidades educativas deben tener en cuenta el rol de los progenitores, o cualquier otra persona que tenga bajo su responsabilidad el cuidado de las niñas, niños y adolescentes, en la formación personal de ellos, que incluye el uso responsable y seguro de internet y las redes sociales digitales. Es tarea del Estado y las entidades educativas proveer información y fortalecer capacidades de los progenitores y personas responsables, sobre los eventuales riesgos a los que se enfrentan las niñas, niños y adolescentes en los ambientes digitales.

2. Toda medida que implique control de las comunicaciones tiene que respetar el principio de proporcionalidad; por tanto, se debe determinar que la misma tiene como fin la protección y garantía de derechos que es adecuada al fin perseguido y que no existe otra medida que permite obtener los mismos resultados y sea menos restrictiva de los derechos.

3. Se debe transmitir claramente a las niñas, niños y adolescentes que internet no es un espacio sin normas, impune o sin responsabilidades. Deben alertarlos para no dejarse engañar con la aparente sensación de que allí todo vale, dado que todas las acciones tienen consecuencias.

Deben ser educados en el uso responsable y seguro de internet y las redes sociales digitales. En particular:

3.1. La participación anónima o el uso de pseudónimos es posible en las redes sociales digitales. El proceso educativo debe reflexionar sobre los aspectos positivos del uso de pseudónimos como medio de protección y un uso responsable que –entre otras cosas– implica no utilizarlos para engañar o confundir a otros sobre su identidad real.

Las niñas, niños y adolescentes deben ser advertidos sobre la posibilidad de que cuando creen estar comunicándose o compartiendo

información con una persona determinada, en realidad puede tratarse de otra persona. Al mismo tiempo, es necesario advertir que la participación anónima o con un pseudónimo hace posible la suplantación de identidad.

3.2. En el proceso educativo es necesario enfatizar el respeto a la vida privada, intimidad y buen nombre de terceras personas, entre otros temas. Es importante que las niñas, niños y adolescentes sepan que aquello que puedan divulgar puede vulnerar sus derechos y los de terceros.

3.3. Los niños, niñas y adolescentes deben conocer que la distribución de contenidos prohibidos por la regulación local y regional (en especial la pornografía infantil), el acoso (en especial el acoso sexual), la discriminación, la promoción del odio racial, la difamación y la violencia, entre otros, son ilegales en internet y en las redes sociales digitales, y están penados por la ley.

3.4. El proceso educativo debe proveer de conocimiento acerca del uso responsable y seguro por parte de las niñas, niños y adolescentes de las políticas de privacidad, seguridad y alertas con las que cuentan los instrumentos de acceso y aquellos sitios web en los que las niñas, niños y adolescentes son usuarios frecuentes como las redes sociales digitales.

3.5. Se debe promover una política educativa -expresada en términos acordes a la edad de las niñas, niños y adolescentes- que incluya una estrategia informativa y formativa que los ayude a gestionar las potencialidades y los riesgos derivados de la Sociedad de Información y el Conocimiento, en especial del uso de internet y de las redes sociales digitales.

3.6. Asimismo, se debe informar sobre los mecanismos de protección y las responsabilidades civiles, penales o administrativas que existen cuando se vulneran derechos propios o de terceros en la red.

3.7. Se debe advertir del peligro que supone el llamado robo 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 de 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, así como de los demás aspectos indicados en el numeral 3.

4.2. La producción de material didáctico, especialmente audiovisuales, páginas web y herramientas interactivas (tales como juegos *online*) en el que se presenten las potencialidades y los riesgos. Estos materiales deberán incluir información acerca de los mecanismos de protección de los derechos. La naturaleza de estos temas y materiales exige de la participación y discusión de los mismos por parte de todos los actores involucrados y con ello responder a las particularidades locales y culturales.

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 organizacio-

nes 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.

Referencias bibliográficas

Barindelli, Florencia (2011), "La protección de datos personales en las redes sociales digitales en particular de niños y adolescentes", *Memorando de Montevideo*, Instituto de Investigación para la Justicia/Instituto Federal de Acceso a la Información y Protección de Datos/Centro de Investigaciones para el Desarrollo.

Barriuso Ruiz, Carlos (2002), *La contratación electrónica*, Madrid, Dykson.

Peschard, Jacqueline (2011), "La protección de datos personales en las redes sociales digitales en particular de niños y adolescentes", *Memorando de Montevideo*, Instituto de Investigación para la Justicia/Instituto Federal de Acceso a la Información y Protección de Datos/Centro de Investigaciones para el Desarrollo.

Piñar Mañas, José Luis *et al.* (2011), *Redes sociales y privacidad del menor*, Madrid, Reus.

Piñar Mañas, José Luis y Lina Ornelas Núñez (2013), *La protección de datos personales en México,* México, Tirant lo Blanch.

Rodotá, Stefano (2011), *Redes sociales y privacidad del menor*, Madrid, Fundación Solventia.

Sitios en internet

Academia KhanAcademy. Disponible en <https://es.khanacademy.org>.

Aprende a Aprender con TIC, Secretaría de Educación Pública. Disponible en <http://tic.sepdf.gob.mx>.

Asamblea Parlamentaria del Consejo de Europa, Recommendation 509 (1968) *on human rights and modern scientific and technological developments*. Disponible en <http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta68/EREC509.htm>.

Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de las Comunidades Europeas* (2000/C 364/01). Disponible en <http://www.europarl.europa.eu/charter/pdf/text_es.pdf>.

Comisión Nacional de Seguridad, comunicado de prensa, núm. 34. Disponible en <http://www.ssp.gob.mx/portalWebApp/appmanager/portal/desk?_nfpb=true&_windowLabel=portlet_1_1&portlet_1_1_actionOverride=%2Fboletines%2FDetalleBoletin&portlet_1_1id=1266035>.

Conclusiones del Abogado General, 25 de junio de 2013, *Google Spain, S.L., Google Inc contra Agencia Española de Protección de Datos (AEPD) y M. C. G.*, Asunto C-131/12. Disponible en <http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=795451>.

Consejo de Europa. Disponible en <http://www.echr.coe.int/Pages/home.aspx?p=home>.

Consejo de Europa. *Convenio para la protección de los niños contra la explotación y el abuso sexual*. Disponible en <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=201&CM=8&DF=&CL=ENG>; <http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm>; <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG> y <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Convenio Europeo de Derechos Humanos. Disponible en <http://www.echr.coe.int/Documents/Convention_SPA.pdf>.

Convention on Cybercrime. Disponible en <http://conventions.coe.int/Treaty/en/Reports/Html/185.htm>.

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse CETS, núm. 201. Disponible en <http://www.conventions.coe.int/Treaty/EN/treaties/Html/201.htm>.

Convención sobre los Derechos del Niño. Disponible en <http://www2.ohchr.org/spanish/law/crc.htm>.

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Disponible en <http://conventions.coe.int/Treaty/EN/Reports/Html/201.htm>.

Cuadernillo Estándares TIC para la Educación Básica en el Distrito Federal. Disponible en <http://tic.sepdf.gob.mx/images/archivos/inicio/estandares_20100622.pdf>.

Declaración de los Derechos del Niño de 1959. Organización de las Naciones Unidas. Disponible en <http://daccess-ddsny.un.org/doc/RESOLUTION/GEN/NR0/145/78/IMG/NR014578.pdf?OpenElement>.

Decreto por el que se adiciona la fracción XXIX-O al Artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_185_30abr09.pdf>.

Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf>.

Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y se reforman los Artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010>.

Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva. Disponible en <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:332:0027:0045:ES:PDF>.

Documento de trabajo del Grupo de Trabajo de la Directiva 95/46/CE, *Privacidad en internet: enfoque comunitario integrado de la protección de datos en línea*, *WP 37*. Disponible en <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp37_es.pdf>.

Estudio Digital Records could expose intimate details and personality traits of millions. Disponible en <http://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions>.

Estudio MKT Digital y Redes Sociales en México 2012. Asociación Mexicana de Internet. Disponible en <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=198&Type=1>.

Good to know. Disponible en <http://www.google.com.mx/goodtoknow>.

Guía del Taller "Prevención contra el delito cibernético", Comisión Nacional de Seguridad. Disponible en <http://www.ssp.gob.mx/portalWebApp/ShowBinary?nodeId=/BEA%20Repository/1214152//archivo>.

Guía práctica para ejercer el derecho a la protección de datos personales. Disponible en <http://inicio.ifai.org.mx/Publicaciones/01GuiaPracticaEjercerelDerecho.pdf>.

Guía práctica para la atención de las solicitudes de ejercicio de los Derechos ARCO. Disponible en <http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf>.

Guidelines for Industry on Child Online Protection. Disponible en <http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-COP.IND-2013-PDF-E.pdf> y <http://www.itu.int/osg/csd/cybersecurity/gca/cop/guidelines/industry/industry.pdf>.

Hábitos de los usuarios de internet en México, 2013. Asociación Mexicana de Internet. Disponible en <http://www.amipci.org.mx/?P=editomultimediafile&Multimedia=348&Type=1>.

InfoDF, *Tu derecho a la privacidad: la protección de tus datos personales*, InfoDF. Disponible en <http://www.infodf.org.mx/capacitacion/publicacionesDCCT/tuderechoalaprivacidad/derechoalaprivacidad.pdf>.

Information and Privacy Commissioner, Ontario, Canada. Privacidad por Diseño. Disponible en <http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD>.

Instituto Nacional de Estadística y Geografía. Disponible en <http://www.inegi.gob.mx/est/contenidos/espanol/temas/Sociodem/notatinf212.asp>.

Instituto Nacional de Tecnologías de la Comunicación, *Hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*, Instituto Nacional de Tecnologías de la Comunicación. Disponible en <http://www.inteco.es/file/O4-7X0FfwOb7HFjdHHpx7Q>.

International Telecommunication Union . Children. Disponible en <http://www.itu.int/osg/csd/cybersecurity/gca/cop/children.html>.

International Telecommunication Union. Educators. Disponible en <http://www.itu.int/osg/csd/cybersecurity/gca/cop/educators.html>.

International Telecommunication Union. Industry. Disponible en <http://www.itu.int/osg/csd/cybersecurity/gca/cop/industry.html>.

It Gets Better Project. Disponible en <www.itgetsbetter.org>.

Journal of Computer-Mediated Communication. Disponible en <http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html>.

Ley de Firma Electrónica del Distrito Federal. Disponible en <http://www.poderjudicialdf.gob.mx/work/models/PJDF/Transparencia/IPO/Art14/Fr01/01Leyes/LeyFirmaElectronica_20110816.pdf>.

Ley de Protección de Datos Personales para el Distrito Federal. Disponible en <http://www.infodf.org.mx/nueva_ley/14/1/doctos/LPDPDF.doc>.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Disponible en <http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf>.

Lineamientos de Protección de Datos Personales. Disponible en <http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf>.

Lineamientos del Aviso de Privacidad. Disponible en <http://dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013>.

Memorandum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes. Memorandum de Montevideo. Disponible en <http://iijusticia.org/Memo.htm>.

Ornelas Núñez, Lina y Samantha Alcalde Urbina, *La seguridad como una pieza clave en el rompecabezas de la protección de datos personales. Retos de la Protección de Datos Personales en el Sector Público,* Instituto de Acceso a la Información Pública y Protección de Datos Personales en el Distrito Federal, diciembre de 2011. Disponible en <http://www.infodf.org.mx/web/comsoc/campana/2012/LIbrodatosPweb.pdf>.

Recomendaciones en materia de seguridad de datos personales. Disponible en <http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013>.

Recommendation of the Council on the Protection of Children Online. Disponible en <http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=272&InstrumentPID=277&Lang=en&Book>.

Secretaría de Finanzas del Distrito Federal. Centros de Servicio @ Digital. Disponible en <http://www.finanzas.df.gob.mx/csDigital/servicios.html>.

Study on monetising privacy. An economic model for pricing personal information, European Union Agency for Network and Information Security (ENISA). Disponible en <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy/at_download/fullReport>.

Svitak, Adora. Disponible en <www.adorasvitak.com>.

Telefónica México, Movistar. Disponible en <http://www.telefonica.com.mx/RC-Sostenibilidad-Como-se-utilizan-las-TIC-Uso-Responsable>.

The right to be forgotten – between expectations and practice. Disponible en <http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport>.

Tood, Amanda. Disponible en <http://www.youtube.com/watch?v=Pc1sK1WX2LA>.

Tribunal Constitucional de España. Pleno. SCT 292/2000, 30 de noviembre de 2000. Disponible en <http://www.tribunalconstitucional.es/es/jurisprudencia/Paginas/Sentencia.aspx?cod=13751>.

University of St. Andrews. Disponible en <http://www.standrews.ac.uk/news/archive/2013/title,223732,en.php>.

YoDIGO. Disponible en <http://yodigo.org.ar>.

Colección Ensayos para la Transparencia de la Ciudad de México

2007

01 **La transparencia y los sujetos no obligados de la rendición de cuentas.** Alberto Aziz Nassif

02 **Archivos gubernamentales: un dilema de la transparencia**. José Antonio Ramírez Deleón

03 **Transparencia y control ciudadano: comparativo de grandes ciudades**. Irma Eréndira Sandoval

2008

04 **¿Por qué transparentar las actividades de cabildeo? El caso del Presupuesto de Egresos de la Ciudad de México.** Alejandra Betanzo de la Rosa

05 **Transparencia y procuración de justicia en el Distrito Federal.** Catalina Pérez Correa González y Alejandro Madrazo Lajous

06 **Acceso a la información y transparencia política en el Distrito Federal.** Issa Luna Pla

07 **El derecho de acceso a la información pública: una herramienta para el ejercicio de los derechos fundamentales.** Paulina Gutiérrez Jiménez

08 **Transparencia y medios de comunicación.** Marco A. Morales Barba

2009

09 **Hacia una nueva arquitectura de la información pública. Información pública y política social en el Distrito Federal.** Eduardo Bohórquez

10 **Legislar en la oscuridad. La rendición de cuentas en la Asamblea Legislativa del Distrito Federal.** Khemvirg Puente

11 **Construir obra pública, edificar ciudadanía.** Miguel Ángel Pulido Jiménez

12 **Las delegaciones y los servicios públicos: una mirada sobre lo que deberíamos saber.** Darío Ramírez Salazar y Gabriela Morales Martínez

2010

13 **Sindicatos y transparencia en la Ciudad de México.** Arturo Alcalde Justiniani

14 **Transparencia 2.0 Nuevos medios digitales y acceso a la información pública en el Distrito Federal, oportunidad para el empoderamiento ciudadano.** Octavio Islas y Mauricio Huitrón

15 **Transparencia y desarrollo urbano en el Distrito Federal.** Emilio de Jesús Saldaña Hernández

2011

16 **La libertad de expresión y el derecho a la información en México: un desafío de nuestros tiempos.** Emilio Álvarez Icaza Longoria

17 **Transparencia y procesos electorales.** Lorenzo Córdova Vianello

18 **Acceso a la información, periodismo y redes sociales, escenarios futuros.** Jenaro Villamil

19 **Transparencia, acceso a la información y participación social en la ciudad de México.** Ricardo Raphael

2012

20 **Acceso a la información y protección de datos personales en el ámbito de la justicia.** Miguel Carbonell

21 **Transparencia y gobierno abierto en el D.F., ¿Para qué?.** Haydeé Pérez Garrido

Instituto de Acceso a la Información Pública
y Protección de Datos Personales del Distrito Federal

Ensayo 24 "La protección de datos personales de menores en la era digital"

Abril 2014

xxxxxxxx xxxxxx xxxxxx
xxxxx xxxxxxxxxx xxxxxxx xxx
xxxxxxxx xxxxxxx xxxxxxxxxx xxxxxxxx
xxxxxxxx xxxxxxx xxxxx

El tiraje fue de 1,000 ejemplares impresos en papel bond de 90 grs. Y forros en couché de 250 grs. Fuentes tipográficas: (Calibri Regular, Calibri Bold, Calibri italic, Myriad ProRegular y Myriad ProSemibold)
Cuidado de la edición: Dirección de Capacitación y Cultura de la Transparencia