INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"LA PROTECCIÓN DE DATOS PERSONALES DE MENORES EN REDES SOCIALES: DESAFÍOS Y RECOMENDACIONES"

PROPUESTA DE INTERVENCIÓN
Que para obtener el grado de MAESTRO en Derecho de las Tecnologías de la Información y Comunicación

Presenta:

Sergio Hernández Ramírez

Asesor:

Dra. Olivia Andrea Mendoza Enriquez

Ciudad de México, junio de 2018.

Autorización de Impresión

C4

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 25 de junio de 2018

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"La protección de datos personales de menores en redes sociales: desafíos y recomendaciones"

Desarrollada por el alumno

Nombre: **Sergio**

Apellido paterno: **Hernández**

Apellido materno: **Ramírez**

Desarrollado bajo la asesoría del:

Dra. Olivia Andrea Mendoza Enríquez

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Patricia Ávila Muñoz
Gerencia de Capital Humano

***Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

Agradecimientos

A mis padres, Mary y Sergio, por su infinito cariño, apoyo y enseñanzas en todos los momentos de mi vida.

A mis hermanos, Ricardo y Rodrigo, por ser mis amigos y la inspiración que me ayuda a superar cualquier problema.

A la Dra. Olivia Andrea Mendoza Enríquez, que me brindó su apoyo y comprensión durante el curso de la Maestría, así como en la elaboración del presente trabajo.

Tabla de contenido

Índice de cuadros

Introducción

En muchas ocasiones, la gran gama de información que se localiza en Internet resulta benéfica para conocer y difundir cualquier dato que sea de nuestro interés, gusto o cualquier otro motivo. Asimismo, los usuarios encuentran una constante entrada y salida de conocimiento, que les permite obtener nuevas experiencias de vida a través de un espacio en el que se sienten con la confianza o seguridad de poder experimentar algo nuevo en su vida, sin valorar por completo las consecuencias de sus actos.

Sin embargo, por este mismo hecho, cualquier persona con acceso a la Red se encuentra expuesta a múltiples riesgos, si la información que comparte en ella se realiza sin tomar las precauciones necesarias para evitarlos.

Desde una perspectiva más específica, cualquier usuario de Internet, con especial mención a los niños[1], está en constante contacto con el desarrollo de las tecnologías de la información y comunicación (TIC), por lo que la gran cantidad de información que comparte, como es el caso de sus datos personales, se encuentra expuesta a mayores peligros de los que ellos imaginan.

Un ejemplo de lo anterior se localiza en las redes sociales, en la que, si el usuario es menor de edad, comparte información sin considerar si ésta pudiera poner en riesgo su vida o su estabilidad psicológica, buscando por parte de las

[1] Si bien en este trabajo se utilizará indistintamente el término niños, menor o niñez y adolescencia, en ambos casos se entenderá conforme a lo establecido por el artículo 1° de la Convención sobre los Derechos del Niño: se entiende por niño todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad, así como lo establecido en los párrafos 40 a 42 de la Opinión Consultiva número OC-17/02 de la Corte Interamericana de Derechos Humanos. Ambos documentos disponibles para su consulta en *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx* y *http://www.corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf* respectivamente.

personas que comparten sus roles sociales reconocimiento, admiración y elogios principalmente.

Si bien es cierto que con esta exposición de información no se busca auto dañarse, también lo es que la publicación de datos personales de manera indiscriminada permite, por un lado, que cualquier persona con acceso a las publicaciones hechas pueda conocer aspectos de la vida privada que tal vez sólo deban ser del conocimiento de algunas cuantas personas y por otro, que el usuario sea sujeto de conductas que pudieran afectar los múltiples aspectos de su vida, de manera física o mental.

Por ejemplo, si un niño, niña o adolescente realiza una publicación en cualquier red social, en la que indique lo que hizo durante el día en el colegio, seguramente dará a conocer el tipo de cosas que le agrada hacer, gustos en alimentos, el nombre de la escuela, su ubicación, el nombre de los amigos con los que convive, el horario en el que acude e incluso una foto suya con otras personas en el colegio.

En ese sentido, cualquier persona podría identificar plenamente a través de esta clase de publicaciones, respecto de uno o varios niños, sus rasgos físicos, sus gustos y preferencias, la ubicación del colegio, el tipo de uniforme que utilizan, el horario en el que se encuentran estudiando, o cualquier otro dato que le permita iniciar algún tipo de conversación a través de la red social, o incluso, en el mundo físico, hecho por el cual podría dar origen a conductas que pudiesen vulnerar la vida del titular de los datos, tales como el acoso virtual, *ciberbullying*, acoso sexual o *grooming* y peor aún, ser objeto de pornografía infantil[2].

Otro caso en el que la publicación de ciertos datos personales en Internet podría poner en riesgo a un menor de edad, se presenta cuando dichas personas o

[2] El concepto de pornografía infantil se encuentra sujeto a diversas opiniones y matices en cuanto a su alcance y objeto de estudio; sin embargo, la definición más común consistiría en “aquel material que incorpore a un menor real en una conducta sexual explícita”. Boldova, Miguel A, *Pornografía infantil en la red. Fundamento y límites de la intervención del Derecho Penal*, México, Ubijus, 2009, p. 29.

terceros comparten en tiempo real su ubicación, a través de redes sociales como Facebook, Twitter, Foursquare, entre otras, ya que con acceso a este tipo de información, cualquier persona podría localizar a algún menor de edad, por medio de los lugares que más frecuenta, los horarios en los que realiza determinada actividad, o incluso el tiempo que acostumbra a pasar fuera de su hogar, lo cual lo haría vulnerable de ser víctima de delitos como robo, secuestro, violación, u homicidio, entre otros.

Es decir, una vez mencionadas algunas conductas que podrían afectar no sólo a menores de edad, sino a cualquier persona que utilice Internet, es claro que el motivo principal por el que se podría vulnerar la seguridad digital, así como la protección de datos personales de los niños, es la publicación de información que les atañe a través de cualquier medio en la Red.

De esta manera, hoy en día las nuevas generaciones van desarrollando mejores aptitudes y habilidades con el uso de las TIC, pero eso no implica que conozcan el gran riesgo que corren al utilizar sus datos personales en las redes sociales de una manera poco adecuada o sin el conocimiento pleno de los alcances que podría desarrollar, en el uso de estas herramientas.

Ahora bien, si tomamos en cuenta que, con el paso del tiempo, formamos parte de una sociedad cada vez más globalizada, tenemos por consecuencia que algunas conductas se repliquen en Internet en un par de segundos, en cualquier lugar del planeta, en tiempo real y en la gran mayoría de ocasiones sin un control específico sobre los contenidos que se comparten en la red de redes.

A partir del uso de las redes sociales por parte de sus integrantes, se publican fotos, videos, datos y demás información personal; sin embargo, la posibilidad de tener y ejecutar un control efectivo de los datos personales que recaban las redes sociales a partir de las publicaciones, es prácticamente nula, de tal manera que violentan la vida privada de los usuarios sin contar con medios eficaces contenidos en leyes para garantizar su protección.

Tales riesgos podrían ser evitados si se tiene conocimiento del funcionamiento y las políticas de privacidad de los diferentes sitios en línea, en especial, de las redes sociales. De ahí la importancia de pretender identificar el

origen, las razones y algunas consecuencias que pueden generarse a partir del uso que se tiene de Internet, y específicamente del caso de las redes sociales digitales.

En ese orden de ideas, mientras mayor sea la cantidad de datos personales que se compartan en Internet, es más factible que el usuario sea sujeto de alguna vulneración en su vida privada, o en el ejercicio de otros derechos, poniéndose en condiciones que pudieran afectarlo, por ejemplo, por discriminación provocando que sea prácticamente nulo el desarrollo y ejercicio de sus demás derechos en sociedad.

Sin dejar de lado que, como cualquier otra actividad, lejos de prohibir el uso de redes sociales por parte de los niños, niñas y adolescentes, resulta mejor promover ciertas medidas o *recomendaciones* que resulten de utilidad para todos los involucrados en este tema, que permitan la protección de los menores, por lo menos en cuanto a sus datos personales.

Con el fin de dar mayor certeza y claridad al lector, en las siguientes líneas podrá encontrar la relación de redes sociales con el imperativo tecnológico, la protección de datos personales en las mismas, las principales situaciones de riesgo o daño a datos personales a las que pueden encontrarse los niños, niñas y adolescentes, actores involucrados en su uso, tipos de información que en ellas se comparte, el Derecho a la Protección de Datos Personales como derecho fundamental y su relación con el interés superior del menor, los antecedentes de este derecho y la protección de datos personales desde distintas familias jurídicas, el marco jurídico internacional y nacional aplicable, los problemas para proteger los datos personales en redes sociales desde una concepción tradicional, los múltiples actores, jurisdicciones y conflictos de competencia de autoridades locales en la materia, así como resoluciones no vinculatorias y resoluciones del grupo de trabajo Artículo 29 en materia de protección de datos en redes sociales, el Memorándum de Montevideo, el análisis de políticas de privacidad en redes sociales, de acuerdo a la zona geográfica y la presentación de recomendaciones que permitan a cualquier persona velar por la protección de dicha información y la factibilidad de su implementación.

Capítulo 1

Imperativo tecnológico y protección de datos personales en redes sociales

Capítulo 1: Imperativo tecnológico y protección de datos personales en redes sociales

1.1. Imperativo tecnológico y redes sociales

El imperativo tecnológico establece que “todo lo que es factible y puede ser hecho, debe ser llevado a cabo”3, es decir, implica la capacidad de llevar a cabo diversas conductas con apoyo en la tecnología que se encuentra hoy en día, e incluso facilita la realización de cualquier hecho posible sin considerar que pudiese ser contrario a la ética o incluso que no esté sujeto a cualquier límite.

No obstante, esta libertad inherente al descubrimiento, a la investigación o al desarrollo de la tecnología, no debe ser entendida como libertinaje que tenga consecuencias dañinas para la sociedad o el medio que lo rodea.

Para evitar secuelas o resultados perjudiciales para cualquier persona en las tecnologías resulta “imprescindible agregarle una gran dosis de prudencia por cuanto la capacidad de actuar desborda la capacidad de prever”4. Esto es, el deber que tiene cada investigador o desarrollador de tecnología de conducirse de manera responsable ante las consecuencias que deriven del resultado de su trabajo, actuando en cada momento de manera ética y no, sin alguna clase de límites, por el simple hecho de que su objetivo sea realizable o factible.

---

[3] González Rodríguez-Arnaíz, Graciano, “El imperativo tecnológico una alternativa desde el humanismo. cuadernos de bioética”, *Revista Cuatrimestral de Investigación,* Madrid, año 2004, volumen XV, núm. 53. enero – abril, *http://aebioetica.org/revistas/2004/15/1/53/37.pdf*

[4] Ramírez B., Edgar Roy, “Crítica al imperativo tecnológico”, *Revista de Filosofía de la Universidad de Costa Rica*, Costa Rica, año 1998, volumen XXXVI, núm. 88/89, P. 431, *http://www.inif.ucr.ac.cr/recursos/docs/Revista%20de%20Filosof%C3%ADa%20UCR/Vol.%20XXXVI/No.88-89/Cr%C3%ADtica%20al%20imperativo%20tecnol%C3%B3gico.pdf*

De tal manera que, con tal de llevar a cabo algo que fue posible debido a la tecnología presente, las consecuencias éticas de las acciones que se verifican, pasan a segundo plano o peor aún no se tienen en cuenta, por las personas que las realizan.

Día a día nos encontramos con el inevitable uso de las TIC en cada una de las actividades en las que interviene el hombre, desde cosas básicas como solicitar transporte, alimentos o incluso reservar algún lugar para dormir, hasta situaciones más complejas como transacciones electrónicas, checar la seguridad de algún inmueble, hasta verificar la geolocalización de cualquiera de nuestros conocidos.

A través de la mejora continua a estos productos y servicios, se presenta una disyuntiva, por un lado, la muy probable vulneración a nuestra vida privada o a la vulneración de la protección de datos personales, por el tratamiento que éstos sufren, y por otro, la necesidad de utilizar las TIC, aparentemente a cualquier costo, con el fin de satisfacer nuestras necesidades cotidianas diariamente.

Así, diversas personas enfrentan una situación que pudiera comprometer su ética como profesional en el uso de datos personales de terceros. Un ejemplo de lo anterior se presenta en casos que involucran el desarrollo de las políticas de privacidad de cualquier red social y su correspondiente aplicación electrónica para dispositivos móviles.

Por tal motivo, el desarrollador de cualquier red social que involucre el tratamiento de datos personales, y más en el caso de menores, debe de contar con un conocimiento de la regulación aplicable al sector de mercado en el que desea participar, llámese Europa, América o de manera global, situación en la que se ahondará más adelante.

No es óbice indicar la relevancia que cobra la implementación de buenas prácticas, acompañado del uso ético de los datos personales, por parte de los administradores y desarrolladores de aplicaciones, sitios web y redes sociales, toda vez que sin demeritar la normativa que pueda existir en la materia, lo cierto es que, en la gran mayoría de ocasiones, el cambio en las conductas de los usuarios proviene a partir de la experiencia y el ensayo-error que se presentan día con día en Internet.

Pareciera que el desarrollo de las múltiples actividades del hombre en la sociedad de la información ha provocado una evolución del homo sapiens al hombre digital u “homo digitalis”5, el cual presenta cada vez más un apego y necesidad a recurrir de la tecnología para realizar sus labores o actividades cotidianas.

Es claro que en los últimos años son los menores quienes tienen mayor acceso a las TIC y al infinito contenido que se ubica en la red de redes. En el caso de México, de acuerdo con datos del Instituto Nacional de Estadística y Geografía, al segundo trimestre de 2016, el 59.5 por ciento de la población de seis años o más en México se declaró usuaria de Internet, es decir 65.5 millones de personas, “de las cuales poco más de la mitad de la población de seis años o más se declaró como usuaria de Internet, entre los individuos de 12 a 24 años, las proporciones son superiores al 80 por ciento, es decir, entre los jóvenes es habitual el uso de Internet”6.

Lo anterior, muestra una situación peculiar que no sólo se presenta en nuestro país, sino cada día acontece en el resto del mundo: Los niños prefieren un celular, tableta electrónica o cualquier dispositivo electrónico en lugar de un juguete tradicional perteneciente al mundo físico y no al ciberespacio.

Esta exposición de los niños y evidentemente de cualquier otra persona que se relacione con ellos, en el ciberespacio permite que, gracias al uso de sus datos personales, (entiéndase como gustos, preferencias, búsquedas, compras, visitas frecuentes a determinados juegos o páginas electrónicas, entre otras) y a las mejoras de su experiencia en el uso de las mismas, permiten que al momento de desarrollar nuevas herramientas electrónicas 1) no existan límites en la capacidad de investigar, y por tanto, tampoco se genere algún límite a la capacidad del saber (Imperativo científico); 2) si todo lo que se puede investigar puede ser hecho,

---

[5] Cendoya, Román, *Revolución del homo sapiens al homo digitalis*. Barcelona, Sekotia S. L. 2013, p. 23.

[6] Instituto Nacional de Estadística y Geografía “Estadísticas a propósito del… Día Mundial de Internet (17 de mayo)”, 15 de mayo de 2017, *http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf*

entonces todo lo que se puede hacer debe ser hecho (Imperativo técnico moral) y 3) todo lo que se hace tiene el derecho a ser usado (Imperativo práctico moral)7.

Frente a la utilización desmedida de la tecnología que puede llegar a romper la ética de cada persona, el imperativo tecnológico conlleva una inversión del proceso moral, teniendo como resultado que “El puede, exige el debe. Es decir, si puede hacerse debe hacerse"8, lo cual implica que la factibilidad llega a ser elevada a un concepto normativo, con el resultado de que cualquier tecnología indica que el poder realizar algo se toma en el sentido que se debe hacer.

Lo anterior, lleva al desconocimiento de límites no naturales, rechazando la consciencia de los límites, se renuncia a ejercer la capacidad ética, descuidando las repercusiones de las consecuencias, situación que, si bien es cierto que se seguirá presentando en el uso de las TIC, también lo es que los usuarios cuentan con la facultad de defender sus derechos y también, cuentan con el deber de tener un uso responsable de las herramientas electrónicas que le permiten interactuar con el mundo.

Langdon Winner propone el denominado "control democrático de la tecnología"9, cuya meta radica en que los regímenes tecnológicos aceptados sean compatibles con los derechos humanos, lo cual conlleva que se deba conservar la capacidad ética respecto del imperativo tecnológico debido a que el hombre no puede obrar sin proponerse fines, mientras que el mundo de la tecnología no contiene indicaciones de fines.

---

[7] González, Graciano, “El imperativo tecnológico, una alternativa desde el humanismo”, *Cuaderno Bioética* Madrid, Universidad Complutense de Madrid, 2004, pp. 39-40, *http://aebioetica.org/rtf/04bioetica53.pdf*

[8] Citado por Ramírez B. Edgar Roy en Crítica al imperativo tecnológico. Revista Filosofía Universidad de Costa Rica, 1998, pp. 430 *http://inif.ucr.ac.cr/recursos/docs/Revista%20de%20Filosof%C3%ADa%20UCR/Vol.%20XXXVI/No.88-89/Cr%C3%ADtica%20al%20imperativo%20tecnol%C3%B3gico.pdf*

[9] Ibídem, p. 431.

Retomando esta idea, bajo la óptica de la dignidad humana que propone Kant, el hombre es el fin, mientras que para la tecnología el hombre puede no ser el fin, sino el medio; por lo que el sistema tecnológico no puede tener una concepción de autonomía absoluta que sí tendría un ser humano, pues la racionalidad implica emitir juicios de valor y normas que el hombre se da a sí mismo, mientras que la tecnología sigue reglas impuestas.

El sistema tecnológico, "incluso no teniendo fines en sí mismo, influye realmente sobre el sistema de fines concretos que el hombre puede perseguir"10.

1.2. Protección de datos personales en redes sociales

Actualmente, se ha generado en la sociedad una necesidad de reconocimiento por cualquier motivo de parte de nuestros familiares, amigos o cualquier persona que tenga contacto con uno mismo en Internet, de tal manera que la promoción de datos personales en Internet es de tal tamaño, que muestra una gran cantidad de información que, en manos de personas con malas intenciones, son una gran fuente de datos para poder llevar a cabo ilícitos dentro o fuera del Ciberespacio.

1.2.1 Principales situaciones de riesgo o daño a datos personales a las que pueden encontrarse los niños, niñas y adolescentes en redes sociales

Respecto de los riesgos a los que cualquier persona puede estar expuesta o puede sufrir en su interacción en Internet, pueden clasificarse de diversas maneras, de las cuales para efectos del presente documento se considera que la más clara es la que aportan Del Río, Sádaba y Bringué en el sentido de clasificar por riesgos pasivos y activos[11].

---

[10] Manzanero Fernández, Delia María. "El Uso Virtuoso De La Tecnología", *Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas*, Madrid, año 2007, núm. 15 (2007-1). *http://pendientedemigracion.ucm.es/info/nomadas/15/deliamanzanero.pdf*

[11] Para dichos autores se puede distinguir a los riesgos pasivos como "aquellas disfunciones que el uso de la tecnología implica, sin que curse necesariamente la

En ese sentido, para efectos de identificar algunos ejemplos de cada clase de riesgos para los niños, niñas y adolescentes, a continuación, se identifican los que se actualizan con mayor frecuencia en la Red y que tienen por consecuencia la vulneración a la protección de datos personales de menores[12]:

Vulneración de derechos de propiedad intelectual: Internet es un mundo lleno de contenidos, mismos que pueden tener un origen legal o no; por lo que el descargar información de manera ilegal, se ha convertido en una práctica común, diversas instancias de la Unión Europea "han acordado la elaboración de una política común sobre los delitos contra la propiedad intelectual"[13].

Es necesario recordar que, durante la navegación en Internet, se realiza un gran intercambio de información, en el que se incluyen datos personales, tales como

---

voluntad de los usuarios" y los riesgos activos "hacen referencia a situaciones en las que disponer de una determinada tecnología facilita que alguien desarrolle una pauta nociva". Del Río, Jorge *et al*., "Menores y redes ¿sociales? De la amistad al cyberbullying". *Revista de estudios de juventud*, España, 2010, núm. 88, p. 115. *http://www.injuve.es/sites/default/files/RJ88-09.pdf*

[12] Cabe señalar que los riesgos identificados se obtuvieron del Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres emitido en marzo de 2009 por el Instituto Nacional de Tecnologías de la Comunicación de España, por lo que, para un análisis mayor de los riesgos mencionados, se recomienda al lector consultar dicho documento, disponible en *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

[13] Instituto Nacional de Tecnologías de la Comunicación de España, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres,* España, 2009, p. 76, *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

la dirección IP[14], cookies[15], nombre, correo electrónico, entre otros, por lo que, al momento de realizar descargas ilegales, aumenta el riesgo de vulneración a la privacidad a través de dichos datos.

[14] La Agencia Española de Protección de Datos, en su informe 327/2003, indicó que la dirección IP "se trata de un protocolo básico de transmisión de datos en Internet, donde cada ordenador se identifica con una dirección IP numérica única. Las redes TCP/IP se basan en la transmisión de paquetes pequeños de información, cada una de los cuales contiene una dirección IP del emisor y del destinatario. […] A su vez, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP." Esto significa que los usuarios de Internet son identificables a través de la dirección IP (estática o dinámica) que utilizan en la Red, por lo que cumple con las características de un dato personal. Agencia Española de Protección de Datos, *Carácter de dato personal de la dirección IP. Informe 327/2003*, España, 2003 *https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf*

[15] De acuerdo con la página electrónica de Microsoft, una cookie es "un archivo de texto pequeño que le ha sido proporcionado por la página web visitada para ayudarle a ser identificado por esa misma página. Las cookies se utilizan para mantener información de estado cuando se exploran diferentes páginas de un sitio Web o volver al sitio Web en un momento posterior". *https://support.microsoft.com/es-es/help/260971/description-of-cookies* Es decir, que por el hecho de consultar de nueva cuenta cualquier sitio electrónico, este archivo permite identificar a la persona para hacer de la navegación en Internet sea más "ágil" y "sencilla" para el usuario, teniendo de por medio que sea automáticamente identificado y que si bien se pueden inhabilitar, lo cierto es que la experiencia del usuario puede ser menos satisfactoria, pero más segura para el titular de sus datos personales.

En ese orden de ideas, el usuario que navegue en cualquier página electrónica tiene al alcance una gran cantidad de información que puede obtener y descargar sin conocer si por ese hecho, podría conllevar a vulnerar derechos de propiedad intelectual o en otros casos, descargar virus o software mal intencionado que pudiera afectar su equipo de cómputo o su dispositivo móvil.

Acceso a contenidos inapropiados: En relación con el riesgo mencionado previamente, durante la navegación en Internet, el menor de edad puede acceder a información que se considera inapropiado para su madurez y desarrollo psicológico, de los que tendrá conocimiento, si al momento de consultar diversas páginas de Internet o a partir de un híper enlace en un correo electrónico, no se cuenta con filtros de contenido, como control parental para navegadores o aplicaciones móviles.

Ejemplos de los contenidos inapropiados o nocivos para los menores son "Contenido de carácter sexual inapropiado, violencia, racismo o contenidos sexistas, anorexia, bulimia o cuestiones estéticas, sectas o terrorismo, contenido que vulnere los valores en que se educa al hijo, contenido falso, inexacto o

---

En ese sentido, la Agencia Española de Protección de Datos ha considerado que este tipo de archivos "permiten el almacenamiento en el terminal del usuario de cantidades de datos que van de unos pocos kilobytes a varios Megabytes" por lo que es considerado un dato personal, por revelar información de la vida íntima o privada de su titular. Agencia Española de Protección de Datos, *Guía sobre el uso de las cookies*, España, 2013, p. 7, *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf*

incierto”[16], así como llevar a cabo conductas que puedan poner en peligro su vida, por ejemplo, el fenómeno denominado “ballena azul”[17].

Acoso virtual y *ciberbullying*: Estas dos conductas, en los últimos años, han aumentado en cantidades impresionantes. Por un lado, tenemos que el acoso virtual o ciber-acoso es aquella conducta por parte de un adulto hacia un menor de edad, en la que lo atormenta, amenaza, hostiga, humilla o molesta mediante Internet, teléfonos móviles, consolas de juegos u otras tecnologías telemáticas.

En cambio, el *ciberbullying* o ciber-acoso entre iguales, es aquella conducta en la que los participantes son menores de edad y en la que principalmente interactúan “en forma de insultos, amenazas o extorsiones”[18]; en el entorno de las tecnologías de la información y comunicación, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños.

Es claro que este tipo de conductas no surgieron a partir del uso cotidiano de la tecnología que tenemos al alcance día con día, sino que a partir de un origen previo, las personas que cometen esta clase de fenómenos sociales, como el

---

[16] Instituto Nacional de Tecnologías de la Comunicación de España, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres,* España, 2009, p. 77. *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

[17] Se trata de un reto dirigido a niños y adolescentes a superar 50 pruebas en la misma cantidad de días, que van desde “despertarse de madrugada a mirar videos de terror, cortarse el brazo con una navaja o acercarse al borde de un precipicio. La última consiste en suicidarse saltando desde un balcón.” Presuntamente creado por Philipp Budeikin. Blasco, Lucía, *Qué es el peligroso juego de "La ballena azul" y por qué preocupa a las autoridades,* BBC Mundo, publicado 26 abril 2017, *http://www.bbc.com/mundo/noticias-39721105.*

[18] Instituto Nacional de Tecnologías de la Comunicación de España, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*, España, 2009, p. 78, *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

"Ciberbullying pasivo (ser insultado por un niño), ciberbullying activo (insultar a otros niños), interacción / chat con desconocidos, tratar con adultos que se hacen pasar por niños, ser insultado por un adulto, citarse a solas con desconocidos"[19], utilizan al Internet como un medio para la reproducción de sus hechos y así alcanzar sus intereses, en la gran mayoría bajo el anonimato.

Acoso sexual o *grooming*: Consiste en las prácticas en línea de adultos "para ganarse la confianza de un (o una) menor fingiendo empatía, cariño, etc. con fines de satisfacción sexual (como mínimo, y casi siempre, obtener imágenes del/a menor desnudo/a o realizando actos sexuales)"[20].

Esta conducta es el preámbulo al daño psicológico y en gran cantidad de ocasiones al abuso sexual de menores, derivando en actividades ilícitas peores como la pederastia o la pornografía infantil, de ahí que estemos en presencia de un factor que aumenta día con día en el ciberespacio y que afecta toralmente a niños, niñas y adolescentes.

Este riesgo se ha desarrollado debido a la inmediatez inherente a las redes sociales que permiten el envío y recepción de mensajes en tiempo real que existen en la Red, para obtener imágenes de "contenido erótico del menor que después utilizará para coaccionarle, bajo amenaza de difundir esas imágenes, y evitar así que la relación se corte"[21] entre el menor y el adulto, afectándolo psicológicamente, así como la evidente vulneración a sus datos personales.

Amenazas a la privacidad: Cualquier persona al momento de utilizar Internet, a través de redes sociales, foros de discusión, correo electrónico, o

---

[19] Ibídem

[20] Obtenido de la página Internet Grooming de la iniciativa Pantallas Amigas, *http://internet-grooming.net/*

[21] Instituto Nacional de Tecnologías de la Comunicación de España, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*, España, 2009, p. 79, *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

cualquier otra aplicación, por lo general comparte información que en principio es personal o íntima, a información de dominio público.

Lo anterior, es realizable a través de diversas conductas, tales como “facilitar datos personales del menor, difusión por terceras personas de imágenes del menor sin conocimiento, que el menor grabe y difunda imágenes inapropiadas.”[22]

Al momento de compartir esta clase de información, o cualquier otra que pueda identificar al emisor, puede poner en riesgo la privacidad del mismo, o de cualquier otra persona que conviva con el titular dichos datos, lo que genera que esta acción pueda comprometer la seguridad de terceros, por ignorancia de los alcances de la exposición de los contenidos, o por querer llevar a cabo ese daño.

Por ejemplo, para el caso de menores de edad, se puede poner en riesgo su seguridad, por el hecho de compartir imágenes con poca ropa de cualquier niño, toda vez que existen programas informáticos que permiten a otras personas utilizar esas fotos para sitios de pornografía infantil; asimismo, compartir los lugares o ubicaciones diarias a los que acuden los menores de edad, el nombre de la escuela en la que estudian, fotos en las que aparezcan con otros niños, entre otra clase de imágenes o videos pueden aumentar en gran medida el nivel del daño que pudiera vulnerar la privacidad del menor, sin mencionar la respectiva configuración de los controles de privacidad que aceptan al momento de utilizar cualquier sitio en Internet.

Sexting: Relacionados con los riesgos indicados, resulta indispensable pronunciarse respecto de esta conducta, consistente en el “envío de imágenes (fotografías o vídeos) con contenido sexual por medio del móvil”[23].

Es claro que las consecuencias que devienen de la transmisión de esta clase de información afecta en primer lugar al titular de los datos que en ella se encuentra representado, ya que forman parte del aspecto íntimo del menor y que si bien desde

---

[22] Ibídem. Pág. 80.

[23] Flores, Jorge. *Sexting: adolescentes, sexo y teléfonos móviles*. Pantallas Amigas, 2009. *http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/sexting-adolescentes-sexo-y-telefonos-moviles.shtm*

un principio, no deberían de existir, al momento de transferirlas a otra persona, pierden el control de su destino y difusión en la Red.

Además, los menores de edad son un sector más que vulnerable al sexting, ya que existen cada vez mayores casos de esta conducta, debido a motivos como la "falta de cultura de privacidad, menor consciencia de los riesgos y exceso de confianza, el despertar sexual y sexualización precoz de la infancia e inmediatez de las comunicaciones"[24].

Si bien es cierto que esta clase de hechos no presentan daños únicamente para los menores de edad que envían esta clase de información, también lo es que las personas que difunden las imágenes con contenido sexual explícito, pueden ser sujetos de delitos que involucren la pornografía infantil, la trata de personas, entre otros, así, resulta doblemente importante inhibir la propagación del sexting entre cualquier persona.

Riesgos económicos y/o fraudes: En principio, podría considerarse que esta clase de riesgos no resultaría relevante para menores de edad, sin embargo conforme a lo establecido en el Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia del 23 de noviembre de 2001, además de ahondar en temas como delitos relacionados con pornografía infantil o delitos de propiedad intelectual, encuadra el fraude informático, en el que a través de medios electrónicos, y con un carácter lucrativo de alguien, se genera perjuicio patrimonial de un tercero que afecta potencialmente a cualquier usuario de Internet[25].

---

[24] Para un mayor estudio y análisis de este riesgo, se recomienda al lector la consulta de la *Guía sobre adolescencia y sexting: qué es y cómo prevenirlo*, emitido de manera conjunta por Instituto Nacional de Tecnologías de la Comunicación de España, el Observatorio de la Seguridad de la Información y Pantallas Amigas, publicado en febrero de 2011, *http://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf*

[25] Artículo 8 del Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia del 23 de noviembre de 2001: Artículo 8. Fraude informático.

Como se ha mencionado líneas arriba, los niños, niñas y adolescentes tienen acceso a través de cualquier dispositivo conectado a la Red, a múltiples contenidos peligrosos en los que se presentan casos en los que los menores "se han visto engañados en el transcurso de una compra o intercambio en Internet ante ofertas aparentemente ventajosas"[26], motivo por el cual se vuelven sujetos de fraudes en el que mayoritariamente participan con patrimonio de sus padres, tutores o de terceros.

Amenazas técnicas y/o malware: Irremediablemente el paso del tiempo permite a diversas personas desarrollar ataques cibernéticos a través de virus, o programas informáticos maliciosos, también denominados malware, en los que a pesar de contar con las últimas actualizaciones de los antivirus o firewall más poderosos del mercado, se puede generar un daño a la información contenida en los dispositivos con los que se navega en la red de redes, de una manera apreciable como el cifrado o borrado de información, así como de manera sigilosa ocultándose y así, le permita obtener información personal del usuario, actividades bancarias e incluso la suplantación de identidad electrónica.

Además, dependiendo del tipo de software que afecte al dispositivo, "la infección puede revelar datos como contraseñas del ordenador atacado o incluso

---

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a) Cualquier introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona, *https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf*

[26] Instituto Nacional de Tecnologías de la Comunicación de España, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres*, España, 2009, p. 81, *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf*

activar la webcam de manera remota"[27] hecho que daría origen a otro tipo de riesgos como los previamente indicados.

Con esta clase de riesgos, se da una pequeña muestra de las probables causas que generarían daños a la esfera jurídica de cualquier persona, y con mayor razón a la de niños, niñas y adolescentes a través de Internet.

1.2.2 Actores involucrados en el uso de en redes sociales

Es importante señalar que el desarrollo tecnológico es algo incontrolable, en cuanto a la rapidez con la que avanza y los alcances que llega a tener gracias a la globalización. Sin embargo, las personas que interactúan con las TIC, deben de estar preparadas para el uso de dichas herramientas en relación con el desarrollo tecnológico mencionado, a partir de una mejor cultura del uso y aprovechamiento de las mismas, junto con un punto de vista ético sobre el mismo, por ejemplo, sin poner en riesgo bienes mayores a la evolución tecnológica, como puede ser el interés superior del niño[28].

Por otro lado, es dable decir que no sólo los usuarios (en este caso niños) son responsables respecto del daño que pueden recibir en su esfera jurídica en relación con sus datos personales, ya que otros actores como sus padres, tutores, amigos, los desarrolladores de redes sociales, los organismos garantes de protección de datos personales o terceros que busquen generar alguna conducta

---

[27] Ibídem P. 82.

[28] Conforme a lo establecido en la Opinión Consultiva número OC-17/2002 del 28 de agosto de 2002 de la Corte Interamericana de Derechos Humanos, en relación con el principio 2 de la Declaración de los Derechos del Niño de 1959 y el artículo 3 de la Convención sobre los Derechos del Niño, se entiende que el Interés Superior del Niño es el "principio regulador de la normativa de los derechos del niño se funda en la dignidad misma del ser humano, en las características propias de los niños, y en la necesidad de propiciar el desarrollo de éstos, con pleno aprovechamiento de sus potencialidades así como en la naturaleza y alcances de la Convención sobre los Derechos del Niño", *http://www.corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf*

relacionada con el derecho de los primeros, son corresponsables en el desconocimiento, mal uso o transmisión de los mismos en redes sociales.

Es decir, cada uno de los mencionados puede llegar a tener dentro de la problemática indicada líneas arriba, una participación que permiten delimitar el grado de responsabilidad de cada uno, así como de la injerencia que podrían llegar a tener en esta clase de acontecimientos (vulneraciones a la protección de datos personales de los niños) que se vuelven más cotidianos, por lo que es imperativo una nueva creación de conciencia entre los involucrados sin perjudicar a los menores, salvaguardando en todo momento el interés superior del menor.

Por lo que se refiere a los niños, son los titulares de los datos personales que se comparten en redes sociales, cuentan con la protección internacional a través del interés superior del menor y debido a que no cuentan con el nivel pleno de madurez psicológica necesario para distinguir entre los riesgos a los que están expuestos o en su defecto, sobre cómo protegerse de los mismos.

En ese sentido, es indispensable su participación activa durante el tiempo que utilizan redes sociales y que directa o indirectamente, se encuentran expuestos a través de la publicación de sus datos personales en Internet, a través de fotos, videos, transmisiones en vivo o incluso por medio de publicaciones que los involucre, hechas por cualquier otra persona.

Su participación radica principalmente en el uso de sus datos personales en redes sociales digitales, ya sea por cuenta de ellos o de un tercero, por lo que el principal afectado por el daño ocasionado a partir del uso de dicha información son los niños, niñas y adolescentes.

Probablemente se presuma que este sector de la sociedad sea el menos responsable de los problemas a los que se exponen día con día en la red de redes; sin embargo, tal y como se identificará líneas adelante, cada uno de los actores pueden tener una participación distinta en la protección de los datos personales de menores en redes sociales.

A su vez, los padres de familia, familiares o tutores son los responsables de la crianza, cuidado, educación y desarrollo del menor, que tendrán como

preocupación fundamental el interés superior del mismo, que encuentren un desarrollo pleno en todos los ámbitos de su vida.

En este punto, resulta necesario recalcar que, debido a las condiciones sociales actuales, la concepción de la familia ha cambiado de ser únicamente tradicional (madre, padre e hijos, y en algunos casos con abuelos o nietos), a otros tipos como la familia en transición, que no cuenta con una de las figuras tradicionales, de tal manera que se encabezan por madres solteras; parejas sin hijos, parejas de adultos cuyos hijos ya no viven con ellos, co-residentes, en la que cohabitan familiares o grupos de amigos sin parejas; y unipersonales, con individuos que viven solos. En tanto, la familia emergente abarca los hogares encabezados por padres solteros; parejas del mismo sexo; y parejas reconstituidas que han tenido relaciones o matrimonios previos, al igual que hijos.[29]

Ahora bien, respecto del derecho a la protección de datos personales por parte de cada tipo de familia indicado en el párrafo anterior, resulta necesario recalcar que la responsabilidad de cada integrante que conviva con el niño, niña o adolescente, consiste en garantizar que se respete y cumpla el interés superior del menor, sin perjuicio de los múltiples factores que influyen en su educación, incluyendo la cultura de la privacidad y sus datos personales.

De esta manera, si bien no es posible acotar la participación de un solo tipo de familia en la vida de los menores de edad y el uso de sus datos personales en Internet, lo cierto es que la Suprema Corte de Justicia de la Nación de nuestro país ha emitido diversos criterios en los que se establecen entre otras cosas, que además del ejercicio de la función educadora y orientadora por parte de los padres o tutores así como de quienes ejerzan el cuidado de los menores, también tienen el derecho y la responsabilidad primordial de promover el desarrollo y el bienestar del niño, y es en ese entorno de crecimiento y transición de las etapas de la infancia y adolescencia hacia la vida adulta, que resulta esencial que cumplimenten su

[29] Obtenido de Boletín UNAM-DGCS-335 *Existen en México tres grupos de familias con 11 variantes: estudio de la UNAM.* Publicado el 15 de mayo de 2017 en *http://www.dgcs.unam.mx/boletin/bdboletin/2017_335.html*

obligación de impartir a los menores la dirección y orientación apropiadas para que éstos puedan ejercer los derechos reconocidos por el sistema jurídico mexicano.[30]

A partir de dicho derecho y deber que tienen los padres, familiares o personas que se encarguen del cuidado de los niños, niñas y adolescentes, éstos podrán contar con un panorama más amplio de las circunstancias físicas y virtuales que los rodean en el ejercicio de sus derechos, como lo es la protección de sus datos personales.

Ellos, al ser los principales actores en la convivencia con los menores de edad, tienen el deber de guiarlos durante sus experiencias en redes sociales, motivo por el cual mientras más conozcan la evolución tecnológica y desarrollo de aplicaciones que puedan usar los niños, contarán con más herramientas para poder salvaguardar su salud física, psicológica y social.

En cuanto a los administradores o creadores de redes sociales, se les debe dar el carácter de responsables de generar medidas de seguridad y privacidad, acordes a los estándares internacionales que permitan a los menores desenvolverse adecuadamente en el uso de sus datos personales en las redes sociales o por lo menos, procuren disminuir lo más posible el nivel de riesgos a los que se pueden enfrentar mediante el uso de la red social digital.

A partir de lo anterior o incluso a partir de las buenas prácticas en la protección de datos personales, deben contar con el conocimiento de los riesgos a que los cualquier usuario, incluidos los niños, niñas y adolescentes, pueden exponerse, para que con el fin de prevenir y disminuirlos, se reflejen en sus

---

[30] Uno de esos criterios se obtuvo de la tesis aislada *Derechos de niñas, niños y adolescentes. el artículo 62 de la ley general relativa, al reconocer el derecho humano a la libertad de religión y conciencia, no vulnera el derecho de los padres a educar a sus hijos conforme a sus propias convicciones.* Tesis 2a. VI/2018 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 50, Tomo I, enero de 2018, p. 537, *https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?ID=2016014&Clase=DetalleTesisBL&Semanario=1*

condiciones de privacidad y medidas de seguridad[31], otorgando mayor confianza a cada uno de sus usuarios respecto del manejo de su información, a partir de su recolección hasta su posterior cancelación.

Dicha situación se vuelve complicada si no cuentan con conocimiento de los riesgos a que los usuarios (y más en el caso de niños, niñas y adolescentes) pueden exponerse por el uso de su red social, aunado al uso que ellos les dan a los datos personales que recaban y por el valor que llegan a adquirir esos grandes ficheros o bases de datos, hecho que debería estar reflejado en sus condiciones de privacidad de manera clara.

Su participación es más que importante, ya que en el desarrollo de las aplicaciones o herramientas contenidas en la red social que hayan creado, se debe llevar a cabo un análisis ético del actuar de los usuarios en razón del funcionamiento de dicha plataforma electrónica; es decir, que no sean los propios administradores o creadores de redes sociales, los que faciliten la vulneración de cualquier tipo a los datos personales de los menores de edad.

No pasa desapercibido que cualquier persona que tenga contacto con datos personales de niños, pueden volverse sujetos activos en la vulneración de su protección de información personal de manera directa o indirecta; es decir, son aquellos que sin tener una relación directa con el menor del cual obtuvo datos personales, deben tener un manejo adecuado de los mismos.

Sobre este punto, se debe tener en cuenta que esto es posible a través de Internet o cualquier otro medio, ya que las personas pueden recabar una gran cantidad de información sobre otras personas, intereses o cosas; sin embargo, para el presente trabajo únicamente nos referiremos a los datos personales de menores de edad.

---

[31] Por mencionar un ejemplo, Facebook cuenta en el vínculo electrónico *https://www.facebook.com/help/safety* con un centro interactivo entre desarrolladores y usuarios, para poder salvaguardar la seguridad de los menores de edad mientras interactúan en la mencionada red social.

Estas personas obtienen información de los menores de edad, de manera directa o indirecta por situaciones o lugares en común que tienen con ellos, tal es el caso de la escuela de sus hijos, negocios como restaurantes o papelerías, o a través de las conexiones que se realizan en las redes sociales, es decir solicitudes de amistad o seguir las cuentas de cualquier usuario de menores de edad.

Así las cosas, dentro de este grupo también se puede localizar a las personas que contratan a menores de edad para efectos de publicidad o cualquier otra clase de trabajo como el modelaje[32].

Situaciones como la anterior puede mostrarse, por ejemplo, en los demás usuarios de redes sociales. Un caso expreso sería el de aquella persona que durante su navegación en Internet o cualquier red social, advierte que existe un probable daño a la seguridad y privacidad de un menor de edad, como puede ser en casos de pornografía infantil, *ciberbullying,* robo de identidad o cualquier otra clase de manejo inadecuado de sus datos personales, obteniendo así el deber de denunciar dichas conductas y en su caso reportarlos conforme a las políticas de privacidad de la red social de las que son usuarios.

Actualmente, la mayoría de la sociedad mexicana considera correcto e incluso como un orgullo compartir información de niños, por ejemplo, datos de identificación a través fotografías y videos de menores en internet, específicamente a través de redes sociales (de manera más focalizada hacia padres e hijos), ya que cada día es más fácil y rápido poder transmitir cualquier información.

---

[32] Resulta necesario señalar que, en la mayoría de los casos, los padres de los menores de edad son quienes promueven esta clase de cuentas en diversas redes sociales, por medio de las cuales exponen múltiples datos personales de sus hijos. Ejemplos de lo anterior se localizan en los siguientes perfiles: *https://www.instagram.com/foreverandforava/* cuenta creada por las madres de ambas niñas; *https://www.instagram.com/kristinapimenova2005/?hl=es-la* cuenta administrada por su representante; *https://www.instagram.com/alonso.mateo/?hl=es* cuenta creada por la madre del menor.

Entre los casos más comunes que se localizan en redes sociales, se ubican las fotos de niños en las que se puede advertir su aspecto físico e incluso datos sensibles, como los que se indicaron líneas arriba, por ejemplo, su religión, datos biométricos, estado de salud, entre otros.

Ciertamente, los padres de familia o tutores no realizan la exposición de sus hijos en las redes sociales, con fines ajenos al orgullo de compartir la experiencia de ser padre en la actualidad y los logros que alcanza el menor en el desarrollo de su vida.

No obstante, es difícil comprobar que cada padre de familia conoce los pasos de configuración mínima de la privacidad de los perfiles en los que comparten información, y en los que probablemente pueden dejar desprotegidos a sus hijos frente a terceros.

Otros datos que se localizan en las publicaciones hechas, son aquellos que permiten identificar el rol social de los niños, niñas y adolescentes tales como su escuela, sus calificaciones, gustos, e incluso otros niños que conviven con ellos, situación que vuelve particularmente peligroso la exposición de su información en Internet, por conductas identificadas como la pornografía infantil, el grooming, bullying, o cualquier otro hecho del mismo tipo.

Además, no debe pasar desapercibido que al final del día se trata de información de los niños y que radica en ellos, el derecho denominado autodeterminación informativa, es decir tienen la facultad de decidir qué datos personales desean compartir y con quién lo desean, de tal manera que los padres o tutores podrían valorar qué tan prudente es publicar fotos o videos que seguramente en un futuro el hijo hubiese deseado evitar.

Al respecto, es necesario hacer referencia a un par de precedentes internacionales en los que se muestra un enfoque respecto del derecho de autodeterminación de los menores de edad, en otros países.

El primer caso, se presentó en Italia en el que básicamente a partir de diversas publicaciones en redes sociales por parte de la madre de un menor,

relacionadas con situaciones familiares que afectaron su desarrollo psicológico y social, éste solicitó tutela contra su madre por tales acciones[33].

Dentro del análisis del caso, se determinó que existen casos en los que las personas de 16 años y en algunos casos de 14 años, cuentan con un amplio margen de autodeterminación, tales como la posibilidad de interrumpir su educación escolar, de trabajar, contraer matrimonio, incluso bajo ciertas condiciones, reconocimiento de sus propios hijos, dar su consentimiento para el reconocimiento de los padres, o para acceder a la interrupción del embarazo.

Así las cosas, el juez determinó, conforme a la petición del menor a través de su tutor, otorgar el permiso correspondiente para estudiar en Estados Unidos a fin de garantizar mayores posibilidades objetivas de desarrollo laboral futuro, sin una opción de marginación social.

Ahora bien, respecto de la difusión de la información que corresponde al menor de edad, el Juez determinó como un deber para proteger al niño y evitar la difusión de información, incluso en el nuevo contexto social al que acudiría, el cese inmediato de la difusión por parte de la madre en redes sociales de imágenes, noticias y detalles relacionados con datos personales y al asunto judicial concerniente al niño[34].

De manera que, el Juez ordenó la eliminación de las redes sociales de las imágenes, información, cualquier dato personal relacionado con el niño y los procedimientos relacionados con el menor, estableció que el tutor debe proceder a

---

[33] La sentencia del expediente 39913/2015 fue emitida por el Tribunal de Roma el 23 de diciembre de 2017 y se encuentra disponible para su consulta en su idioma original en http://www.altalex.com/~/media/altalex/allegati/2018/allegati%20free/tribunale_roma_ordinanza_23_dicembre_2017%20pdf.pdf

[34] Montalto, Lillo, “Sentenciada a pagar 10 mil euros a su hijo si publica fotos suyas en Facebook”, *Euronews,* Italia, 9 de enero de 2018, http://es.euronews.com/2018/01/09/sentenciada-a-pagar-10-mil-euros-a-su-hijo-si-publica-fotos-suyas-en-facebook.

la solicitud de desindexación de los motores de búsqueda, a la cancelación de imágenes, información y cualquier dato relacionado con el niño en las redes sociales, así como advertir también a terceros para que se abstengan de su difusión, incluidos los medios de comunicación, de imágenes, información y cualquier dato relacionado con el niño.

Es sumamente importante señalar que el Tribunal de Roma estableció como multa para los padres del menor que, en caso de publicar cualquier información del menor, debían pagar la cantidad de diez mil euros.

En este caso, es dable presumir que el menor de edad no consintió la publicación de información relativa a situaciones familiares que le generaban circunstancias que dañan su desarrollo psicológico y social, motivo por el cual, se otorgó como medida precautoria, la eliminación de los datos y la prohibición de publicar esa clase de información incluso por su madre.

Este precedente muestra la posibilidad del ejercicio de sus derechos, incluido el relativo a la autodeterminación informativa internacionalmente, con el fin de proteger su desarrollo pleno, con el seguimiento y cuidado de un tutor. Sin embargo, no debe pasar desapercibido que este caso, derivó de la Ley de Derecho de Autor respecto de la imagen de una persona que conforme a la normativa de Italia “no podrá ser exhibido, reproducido o comercializado sin su consentimiento"[35]

[35] Ibídem.

Al respecto, se hace del conocimiento del lector el mencionado artículo 96 de la Ley N° 633 de 22 de abril de 1941 sobre la Protección del Derecho de Autor y los Derechos Conexos, en su idioma original y su traducción al español: 96. Il ritratto di una persona non può essere esposto, reprodotto o messo in comercio senza il consenso di questa, salve le disposizioni dell’articolo seguente. Dopo la norte della persona ritrattata si applicano le disposizioni del secondo, terzo e quarto comma dell’art 93. (original) disponible para su consulta en: *http://www.wipo.int/wipolex/es/text.jsp?file_id=301483.*

No obstante, dentro de la misma normativa italiana, se encuentra el Código sobre la Protección de Datos Personales[36], en el que se establece, de manera similar al marco jurídico mexicano, los principios correspondientes al tratamiento de datos personales, así como al ejercicio de derechos ARCO y en su caso, los medios de defensa con los que cuenta el Titular de los datos, ante la Autoridad Garante de la protección de datos personales en Italia, por lo que también es probable que el menor de edad pudiese proteger su información a través de dicha vía legal.

Otro precedente relacionado con la autodeterminación de menores de edad, se presentó en Austria[37], en la que una joven mayor de edad entabló un juicio en

---

96. El retrato de una persona no puede ser exhibido, reproducido o puesto a la venta sin el consentimiento de esa persona, sin perjuicio de las disposiciones del siguiente artículo.

Después de la muerte de la persona retirada, se aplican las disposiciones de los párrafos segundo, tercero y cuarto del artículo 93. (traducción propia al español).

[36] Disponible para su consulta en *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248*

[37] Es importante hacer del conocimiento del lector que no fue posible localizar la sentencia del presente caso; sin embargo, se localizaron diversas fuentes de consulta en Internet que versan sobre el presente asunto y que a continuación se indican: Cagnazzo, Raffaella, *Austria, dieciocho años, denuncia a sus padres por fotos publicadas en Facebook*, 15 de septiembre de 2016, Corriere della Sera, disponible para su consulta en http://www.corriere.it/esteri/16_settembre_15/austria-diciottenne-denuncia-genitori-foto-postate-facebook-2ceb737a-7b46-11e6-ae27-bc43cc35ec72.shtml, Sputnik News, *Una estudiante de 18 años de Carintia, Austria, ha demandado a sus padres por… subir sus fotos a Facebook sin su consentimiento*, Sputnik News, 20 de septiembre de 2016, disponible para su consulta en https://mundo.sputniknews.com/sociedad/201609201063569194-austria-carintia-facebook-privacidad/, Montalto, Lillo, *Sentenciada a pagar 10 mil euros a su hijo si*

contra de sus padres, debido a la publicación de fotos suyas en la red social Facebook. En este caso, los retratos de la menor de edad la reflejaban en momentos privados e íntimos, situación que después de haber solicitado a sus padres, la eliminación de dicha información, ante la falta de apoyo de los mismos, la joven decidió actuar por la vía legal para lograr sus pretensiones.

Si bien se desconoce hasta la fecha si este caso ha sido resuelto en definitiva, lo cierto es que, las consecuencias de lo determinado por las autoridades del mencionado país, podrían cambiar el paradigma consistente en la publicación de información de menores en redes sociales, desde fotos, videos, audios o cualquier otro tipo de contenido que pudiese afectar la vida privada o intimidad del menor y del cual sus padres podrían ser responsables.

Otro dato relevante consiste en que el presente caso se resolverá a la luz de la legislación austriaca sobre protección de datos, la cual podría traer como consecuencia que los padres tengan que pagar una multa de 3000 a 10000 euros.

Por lo anterior, es probable que en otros países se presenten casos similares respecto del tratamiento de los datos personales de menores de edad, por parte de sus padres, en los que los primeros consideren que actuaron de manera irresponsable y puedan ser sujetos a demandas conforme a la normativa aplicable en materia de protección de datos personales.

Es claro que, si bien en la actualidad suena poco probable que un hijo demande a sus padres por la publicación de sus datos personales en redes sociales, no hay que olvidar que cada día la tecnología permite recabar mayor información y almacenarla en diferentes dispositivos vinculados a internet. Por tal motivo, no se debe descartar la posibilidad que en México o en otros países cuyo sistema jurídico pertenezca al derecho continental, se presenten casos en los que se obligue a los padres o tutores de los menores a eliminar cualquier dato personal del menor por

---

publica fotos suyas en Facebook, Euronews, Italia, 9 de enero de 2018, disponible para su consulta en http://es.euronews.com/2018/01/09/sentenciada-a-pagar-10-mil-euros-a-su-hijo-si-publica-fotos-suyas-en-facebook.

una exigencia del mismo, en atención a su derecho a la autodeterminación informativa.

En este caso, la sociedad en general se encuentra muy familiarizada con la exposición de información en cualquier momento, gracias al avance tecnológico que se tiene en las TIC.

Por ejemplo, la cantidad tan amplia de móviles inteligentes que existen hoy en día, permite a los usuarios de Internet poder cargar y compartir información a través de la red de redes en cuestión de segundos, por lo que una foto, un video o cualquier otro tipo de información que hagan identificable al menor, puede cambiar de posesión con tan solo pulsar un botón.

Asimismo, los autorretratos[38] se han vuelto día a día una práctica común, por medio del cual, a través de un teléfono móvil, una persona puede fotografiarse en cualquier momento y a su vez es muy factible que comparte con quien desee, dicho documento.

Respecto de los creadores o administradores de las redes sociales, se ha desarrollado la inquietud de promover mejores condiciones de privacidad o la posibilidad de identificar plenamente los alcances de compartir información con cualquier persona que se desee.

En este sentido, los actores indicados previamente han llevado a cabo diferentes campañas contra las conductas que ponen en peligro a los menores, tales como programas de control parental, posibilidad de denunciar sitios electrónicos o páginas que se consideran de alto riesgo, campañas de conciencia sobre la carga de información de menores y cambios en sus condiciones de privacidad respecto al cuidado de sus datos personales.

Sitios de redes sociales como Facebook, Twitter, Instagram y Tumblr han cambiado las “reglas del juego” del pornógrafo, aquel que publica material obsceno. Estos sitios ahora ofrecen poderosas herramientas para que los pedófilos dejen de intercambiar imágenes de pornografía infantil a través de las redes digitales, así como para que lo involucrados en esta clase de conductas en Internet sean

[38] Usualmente conocidos como “selfies” por su traducción al idioma inglés.

detectados por los usuarios o administradores y denunciados ante las autoridades correspondiente[39].

De ahí que las autoridades competentes en materia de datos personales de menores deben demostrar necesariamente su interés, preocupación y sobre todo su actuar, respecto de la necesidad que existe por garantizar los derechos de los menores, entre los cuales está la protección de sus datos personales.

En el caso en particular de los niños, los riesgos se generan a partir de los múltiples accesos con los que cuentan hacia las redes sociales, en específico a contenidos que la mayoría de las personas consideran inadecuados por su edad; otro riesgo se identifica a partir del contacto directo que un menor puede tener vía electrónica y posteriormente de manera física con usuarios malintencionados de redes sociales.

La publicación (exposición) de una gran cantidad de información que contiene datos personales de los menores, que se publica por ellos mismos o por terceros se lleva a cabo con desconocimiento de los múltiples riesgos a los cuales pueden ser expuestos.

Estas y otras circunstancias se prestan para que los menores se encuentren frente a posibles riesgos como trata de personas, abusos, extorsión, discriminación, pornografía infantil, amenazas y otros que pueden incidir de manera negativa en su crecimiento y desarrollo armónico e integral, situación que debe garantizar en todo momento el Estado.

---

[39] Ejemplo de esto se ha presentado en España, donde los administradores de las redes sociales digitales implementan Big Data para detectar patrones en las imágenes que se cargan en Internet con diversas características como la cantidad de piel desnuda que existe en ellas y en su caso, las elimina de manera automática si no concuerdan con los parámetros indicados por los algoritmos establecidos para el uso de Big Data. Tomado de Ediziones, Portaltic, *Así combaten la pornografía infantil las principales redes sociales*, Portal TIC/Europa Press, 14 de marzo de 2017, *http://www.europapress.es/portaltic/socialmedia/noticia-asi-combaten-pornografia-infantil-principales-redes-sociales-20170314085947.html*

Finalmente, la Autoridad (Estado) es el responsable de garantizar los derechos fundamentales de todas las personas, tienen un rol vital por el cumplimiento de este deber. En el mundo existen múltiples organismos[40] que se encargan de la protección de los datos personales, en los que tal vez sus atribuciones sean desiguales o su manera de trabajar tengan enfoques completamente distintos; sin embargo, el objetivo es el mismo, velar por la protección de los datos personales.

Así, los responsables de los datos personales llevan a cabo un tratamiento de datos personales ya que los almacenan, procesan o comercializan, a partir de grandes bases de datos que contienen información que adquiere gran valor sí llegan a aprovecharlos para ofrecer bienes o servicios, incluyendo estrategias de negocios.

1.2.3 Tipo de información que se comparte en redes sociales

Ahora bien, se realizó una observación de las prácticas más comunes en redes sociales por parte de diversos usuarios, principalmente respecto del manejo de datos personales de menores.

---

[40] En el caso de México se encuentra el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales cuya misión es "Garantizar en el Estado mexicano los derechos de las personas a la información pública y a la protección de sus datos personales, así como promover una cultura de transparencia, rendición de cuentas y debido tratamiento de datos personales para el fortalecimiento de una sociedad incluyente y participativa" (obtenido de *http://inicio.inai.org.mx/SitePages/misionViosionObjetivos.aspx*). No obstante, uno de los principales entes en la materia es la Agencia Española de Protección de Datos, es la autoridad estatal de control independiente encargada de velar por el cumplimiento de la normativa sobre protección de datos. Garantiza y tutela el derecho fundamental a la protección de datos de carácter personal de los ciudadanos en España (obtenido de *http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php*).

Así, se identificó que dentro de las diversas redes sociales que existen y que probablemente se desarrollen en un futuro, ya sea vía computadoras o en aplicaciones móviles en teléfonos inteligentes, la publicación que realizan los menores y terceros respecto de sus datos personales, resulta la principal causa por el que puede ser expuesta este tipo de información, sin tener plena certeza del nivel de difusión que pueda tener cualquier publicación, ni de las demás consecuencias que podrían generarse.

En las redes sociales se publica información concerniente, entre otras cosas a datos personales de menores, que en la mayoría de ocasiones se realiza sin autorización de los titulares de dichos datos, con afán de obtener el reconocimiento de los demás usuarios, así como por el gusto y muestras de afecto que quieren demostrar frente a cualquier persona que conozca esa información, o cualquier otro motivo que genere su exposición.

Dentro de la observación ya indicada se localizaron diversos tipos de información personal que se localiza en redes sociales y que, sin importar el tiempo transcurrido, permanecen disponibles en Internet, tal y como a continuación se enunciará.

En un primer caso, nos encontramos ante una red social que, hasta junio de 2017, contaba con 2000 millones de personas activas cada mes, es decir Facebook[41]. De acuerdo con su política de datos[42], los tipos de datos que se recopilan son diferentes en función del servicio que se utilice dentro de esta red social. En la siguiente tabla se esquematizará los tipos de datos y uso al que corresponde de todos sus productos y servicios, de acuerdo con la política indicada.

---

[41] De acuerdo con sus últimas estadísticas de la comunidad que utiliza dicha red social, *https://investor.fb.com/home/default.aspx*

[42] La versión completa de esta política se encuentra *https://www.facebook.com/full_data_use_policy*; no obstante, Facebook diseñó una página que permite entender de una manera más clara los datos que recopila de sus usuarios, *https://www.facebook.com/about/privacy/*.

Cuadro 1. Tipos de datos personales utilizados en Facebook.

Servicio o producto de Facebook[43]	Datos que recopila Facebook
Abrir alguna cuenta, crear o compartir contenido y comunicarse con otras personas.	Todos los incluidos en el contenido proporcionado (lugar o fecha de creación), así como aquella información que derive del modo en el que se usan los servicios, como frecuencia o duración de las actividades
Publicaciones de terceros que se relacionan con otro usuario o que contienen datos sobre éste.	Del contenido que se relacione con un usuario, o que incluya sus datos, se recopila desde que se etiqueta a alguien en alguna publicación, se envía mensajes o te identifica como contacto, incluyendo tu información como nombre, correo electrónico o teléfono.

[43] Cabe señalar que dentro de la política de datos de Facebook no se identifica de manera expresa cuáles son todos los servicios y productos de esta red social, sin embargo, dentro del apartado de servicio de ayuda de su página de Internet, se identificó la pregunta ¿Cuáles son los servicios de Facebook? A la que su respuesta consiste en que Facebook proporciona una amplia variedad de productos y servicios, incluidas plataformas de publicidad y comunicaciones tales como aplicaciones para celulares (como Facebook y Messenger). Por otro lado, servicios como ser administrador de páginas o las estadísticas del público, son productos que ofrecen a sus socios comerciales, como los anunciantes. De cualquier modo, todos estos servicios se rigen por su Política de datos, desde su recopilación, uso y divulgación de la información otorgada por el usuario, sin omitir que, en algunos casos, los productos y servicios de Facebook disponen de sus propias condiciones y políticas de privacidad, por lo que podrían tener supuestos diversos a la política principal, *https://www.facebook.com/help/1561485474074139.*

Uso de redes y conexiones con otras personas.	Información sobre los contactos que se tiene cualquier tipo de comunicación, así como aquella que se importe desde algún dispositivo como puede ser una libreta de direcciones o imágenes.
Pagos realizados en Facebook.	Datos de la transacción o compra, tales como número de tarjeta de crédito o débito, datos de la cuenta, autenticación, detalles de facturación, envío y contacto.
Conexión mediante diversos dispositivos.	Información de todos los dispositivos o computadoras que tienen acceso a los servicios de Facebook, tanto la que generan, como sus atributos (sistema operativo, la versión de hardware, la configuración del dispositivo, los nombres y tipos de software y de archivos, la carga de la batería, la intensidad de la señal y los identificadores de dispositivos), ubicaciones del dispositivo, incluida la posición geográfica específica obtenida a través de señales de GPS, Bluetooth o wifi, nombre del operador de telefonía celular o proveedor de servicios de internet, el tipo de navegador, el idioma y la zona horaria, el número de celular y la dirección IP.
Información de los sitios web y las aplicaciones que usan los servicios	Datos de los sitios electrónicos y aplicaciones que se visitan mediante

	Facebook, datos del desarrollador, editor de la aplicación que proporcionan al usuario o a la red social.
Información acerca de los socios de Facebook.	Datos que socios de Facebook recaban del usuario dentro y fuera de la red social, como la relacionada en cuanto a la experiencia o interacciones que se generaron.
Información de las demás empresas de Facebook	Recibe toda aquella información recabada por empresas de Facebook o administradas por esta red social, conforme a sus condiciones y políticas.

De lo anterior, es posible advertir que no hay una lista clara ni estrictamente definida de todos los datos que Facebook recaba de sus usuarios, conforme a su política correspondiente. No obstante, de la observación realizada fue posible identificar que los usuarios crean o comparten una gran cantidad de información en esta red social, y que dentro de los datos personales que se comparten, se encuentra el nombre, domicilio, teléfono, datos de familiares, escuela en la que estudiaron, historial laboral, edad, nacionalidad, estado civil, gustos, preferencias, ubicaciones de los lugares que frecuentan, así como la dirección de otras redes sociales en las que pueden ser localizados.

Por otro lado, también existen usuarios que publican datos personales sensibles suyos o de terceros, como origen racial o étnico, la religión que profesan, estado de salud, afiliación sindical, opiniones políticas, preferencias sexuales, entre otros como los datos biométricos que se pueden obtener a través de las imágenes que se suben a esta red social[44].

[44] Aunque fue posible advertir que en diversos perfiles alrededor del mundo la idiosincrasia es muy volátil, lo cierto es que se identificaron grupos o páginas dentro de Facebook que hacen referencia a cualquiera de este tipo de datos personales.

Otra red social que también recopila datos personales es Instagram, la cual hasta septiembre de 2017 contaba con 800 millones de usuarios mensualmente[45], y que desde 2012 fue adquirido por Facebook. De acuerdo con su política de privacidad, dentro de la información que se recopila, se encuentra el nombre de usuario, contraseña y dirección de correo electrónico al momento de registrarse en una cuenta de Instagram, así como la contenida en el perfil de usuario (por ejemplo, nombre y apellidos, foto, número de teléfono).

Cabe señalar que a diferencia de Facebook, Instagram es una red social que consiste principalmente en compartir imágenes y videos, la exposición de datos personales se realiza principalmente en cada publicación que se realiza, y que puede ser la propia imagen del usuario y demás personas que lo acompañan, sin omitir la demás información que se puede recopilar como la ubicación o demás datos que se agreguen mediante las denominadas etiquetas o *hashtags* que se utilicen al momento de hacer la publicación.

En otras redes sociales como Twitter, Snapchat, Pinterest, LinkedIn y Google+, el contenido de información que se comparte es muy similar a la ya indicada líneas arriba, es decir, dentro de los datos personales que se comparten, principalmente se localizan el nombre, edad, sexo, domicilio, teléfono, trabajo, gustos, intereses, fotos y demás información que pueda identificar a cada usuario.

Además, es claro que cada red social cuenta con un origen distinto a la otra, situación que permite a una misma persona tener una cuenta o perfil dentro de cada una, generando así una identidad digital dentro de Internet, en la que se crea y comparte gran cantidad de información con millones de personas que también utilizan redes sociales.

Incluso, en el caso de México, ha aumentado el uso de redes sociales, como es el caso de Facebook, para demostrar su pertenencia a algún partido político o expresas sus creencias religiosas.

[45] De acuerdo con las últimas estadísticas de la comunidad, *https://investor.fb.com/home/default.aspx*

Ahora bien, dentro del marco jurídico mexicano, el consentimiento para aceptar el tratamiento de datos personales por parte de cualquier responsable, debe ser otorgado por el Titular de los mismos, esto conforme a lo establecido en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[46].

En este caso, las redes sociales que utilizan datos personales de menores deben recaban el consentimiento de sus titulares, conforme a la Ley indicada en el párrafo anterior.

No obstante, en este caso se presenta una problemática: ¿Quién debe dar la autorización para el tratamiento de datos personales y por qué? Aunado a ¿quién es el titular de dicha información?

Al respecto, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece en su artículo 89, entre otras cosas, que "Para el ejercicio de los derechos ARCO (acceso, rectificación, cancelación y oposición) de datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se

[46] Artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición. Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley. El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

estará a las reglas de representación dispuestas en el Código Civil Federal."[47] Así las cosas, dicho cuerpo normativo en su artículo 23,establece que la minoría de edad, es una restricción a la personalidad jurídica que no debe menoscabar la dignidad de la persona, pero que pueden ejercitar sus derechos o contraer obligaciones por medio de sus representantes[48].

[47] Artículo 89 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

[48] Artículo 23.- La minoría de edad, el estado de interdicción y demás incapacidades establecidas por la ley, son restricciones a la personalidad jurídica que no deben menoscabar la dignidad de la persona ni atentar contra la integridad de la familia; pero los incapaces pueden ejercitar sus derechos o contraer obligaciones por medio de sus representantes. Código Civil Federal

Es decir, los niños, niñas y adolescentes únicamente pueden ejercer sus derechos y contraer obligaciones a través de sus padres[49], tutores[50] o quienes ejerzan la patria potestad[51].

Lo anterior resulta contradictorio, debido a que el ejercicio de derechos ARCO, conforme a la normativa aplicable en la materia corresponde al titular de los datos personales, pero en el caso de los menores de edad, restringe su ejercicio únicamente a sus representantes, por lo que para el autor, resulta contradictorio que un derecho que deriva de la autodeterminación informativa, sea limitado por una norma federal, dado que considera al niño, niña o adolescente como incapaz de ejercer sus derechos o contraer obligaciones.

---

[49] Lo anterior, conforme al artículo 414 del Código Civil Federal. La patria potestad sobre los hijos se ejerce por los padres. Cuando por cualquier circunstancia deje de ejercerla alguno de ellos, corresponderá su ejercicio al otro. A falta de ambos padres o por cualquier otra circunstancia prevista en este ordenamiento, ejercerán la patria potestad sobre los menores, los ascendientes en segundo grado en el orden que determine el juez de lo familiar, tomando en cuenta las circunstancias del caso.

[50] Conforme a los artículos 449 y 450, fracción I del Código Civil Federal: Artículo 449.- El objeto de la tutela es la guarda de la persona y bienes de los que no estando sujetos a patria potestad tienen incapacidad natural y legal, o solamente la segunda, para gobernarse por sí mismos. La tutela puede también tener por objeto la representación interina del incapaz en los casos especiales que señale la ley.
En la tutela se cuidará preferentemente de la persona de los incapacitados. Su ejercicio queda sujeto en cuanto a la guarda y educación de los menores a las modalidades de que habla la parte final del artículo 413.
Artículo 450.- Tienen incapacidad natural y legal: I. Los menores de edad; […]

[51] De acuerdo con lo indicado en el Artículo 414, segundo párrafo del Código Civil Federal: Artículo 414.- […] A falta de ambos padres o por cualquier otra circunstancia prevista en este ordenamiento, ejercerán la patria potestad sobre los menores, los ascendientes en segundo grado en el orden que determine el juez de lo familiar, tomando en cuenta las circunstancias del caso.

Así las cosas, considero que, en el caso de los menores de edad, ellos siempre serán los titulares de los datos personales que se traten en internet y especialmente en redes sociales; sin dejar de mencionar, que los padres podrían orientar y en su caso indicarle al menor de edad las consecuencias de cualquier tipo que podría tener publicar algún dato personal suyo.

Para garantizar el cumplimiento de este derecho fundamental, el Estado podría exceptuar, de acuerdo a ciertas circunstancias del caso en concreto, la limitación que establece el Código Civil Federal, para que el menor ejerza sus derechos ARCO y así se salvaguarde su derecho de protección de datos personales.

1.2.4 El Derecho a la Protección de Datos Personales como derecho fundamental y su relación con el interés superior del menor

Respecto del ejercicio de su derecho fundamental a la protección de datos personales, en el que evidentemente se incluye el otorgamiento de la autorización para el tratamiento de dicha información, me parece que conforme al derecho de autodeterminación informativa[52], el niño puede decidir sobre quién y para qué puede utilizar sus datos personales.

Lo anterior no debe ser considerado en estricto sentido, toda vez que existen factores como el interés superior del menor, el cual incluye su desarrollo físico, psicológico y social, del cual sus padres o la persona que tenga la patria potestad,

[52] Es decir, aquella facultad del individuo de decidir por sí mismo sobre la difusión y utilización de sus datos personales, basado en el derecho general de la personalidad y que ofrece protección frente a la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos de carácter personal y «garantiza la facultad del individuo de decidir básicamente por sí mismo sobre la difusión y la utilización de sus datos personales. Martínez, Ricard. “El derecho fundamental a la protección de datos: perspectivas.”, *Revista de Internet, Derecho y Política,* España, III Congreso Internet, Derecho y Política, núm. 5, 2007, p. 48, *https://dialnet.unirioja.es/descarga/articulo/2372613.pdf*

incluido el propio Estado, que deben ser tomados en cuenta para el ejercicio de su derecho de protección de datos personales.

En mi punto de vista, cada situación amerita un análisis casuístico, el cual deberá requerir de un ejercicio de ponderación, por lo que es necesario hacer referencia a la Teoría de derechos fundamentales de Robert Alexy, misma que se apoya en un concepto material de norma jurídica que es de carácter doble, ya que se define por los rasgos propios de los principios, por un lado, en consonancia con la idea de argumentación correcta.

Sin embargo, por otro lado, sigue teniendo peso la validez jurídica de las normas que contienen derechos fundamentales, consideradas como reglas constitucionales. Este carácter doble de la teoría de Alexy permite distintos acercamientos, positivistas y no positivistas.

Ahora bien, en la Teoría de ponderación que se encuentra en el derecho continental se indica que todas las autoridades conforme a los diversos tratados internacionales en materia de derechos humanos, para resolver un conflicto entre principios constitucionales deben establecer una jerarquía entre dos derechos en conflicto, a lo cual se le denomina ponderación o balance.

Sin embargo, previo al análisis para los que se pretende demostrar en el presente documento, es necesario dar una breve referencia a esta teoría dentro del derecho constitucional alemán, la “ponderación expresa optimizar en relación con un principio de colisión no consiste en otra cosa que ponderar. La ley de ponderación muestra que ésta puede descomponerse en tres pasos. En el primero debe constatarse el grado de incumplimiento o perjuicio de un principio. A él debe seguir en un segundo paso la comprobación de la importancia de la realización del principio contrario. En un tercer paso finalmente debe averiguarse si la importancia de la realización del principio contrario justifica el perjuicio o incumplimiento del otro”[53]

[53] Alexy, Robert. “Derechos fundamentales ponderación y racionalidad”, *Revista Iberoamericana de Derecho Procesal Constitucional*, México, 2009, núm. 11, enero-junio de 2009, p. 9. Originalmente publicado como “Grundrechte, Abwägung und

Es decir, frente al choque de derechos que se genera en una situación determinada, la autoridad debe constatar primero la vulneración o no aplicación de un derecho fundamental frente a otro, que a su vez sea trascendental dicha inobservancia para que finalmente se determine si ésta resulta ser adecuada por el incumplimiento o no aplicación del segundo derecho que resultó tener un ejercicio nugatorio.

De esta manera los derechos del menor, o también denominados derechos del niño, los conceptualiza Jiménez como un "derecho singular, eminentemente tuitivo, que tiene por objeto la protección integral del ser humano, desde su concepción hasta que alcanza, tras su nacimiento, la plena capacidad de obrar, que se inicia con la mayoría de edad, para integrarle armónica y plenamente en la convivencia social"[54].

Así, por medio de la regulación que otorga el Derecho, es dable considerar que el Estado debe propiciar el desarrollo integral del menor, de tal manera que no pueda vulnerarse en cualquier ámbito de su vida, toda vez que en cualquier momento debe privilegiarse el interés superior del menor.

Doctrinalmente el interés superior del niño implica que en todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de

---

Rationalität", en Ars Interpretandi. Yearbook of Legal Hermeneutics, Münster, Lit, núm. 7, 2002, pp. 113-125. Versión inglesa del propio autor: "Constitutional rights, balancing, and rationality", en Ratio Juris, Oxford, Ing.-Malden, EUA, Universidad de Boloña, vol. 16, núm. 2, junio de 2003, pp. 131-140. Traducción española anterior de David García Pazos y Alberto Oehling de los Reyes, con el mismo título que la presente, en Fernández Segado, Francisco (ed.), The Spanish Constitution in the European constitutional context. La Constitución española en el contexto constitucional europeo, Madrid, Dykinson, 2003, pp. 1505-1514, *http://www.corteidh.or.cr/tablas/r25294.pdf*

[54] Jiménez García, Joel Francisco, *Derechos de los niños*, México, Instituto de Investigaciones Jurídicas, 2000, p. 4 y 5, *http://biblio.juridicas.unam.mx/libros/1/69/tc.pdf*

bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial que se atenderá, será el interés del menor[55].

No obstante, al ser el niño un integrante toral de la sociedad, el cual puede llegar a tener un rol distinto de acuerdo al ámbito en el que se desarrolle, la conceptualización de la multicitada figura jurídica deberá ser entendida y orientada según la materia de que trate la convención internacional o normativa nacional aplicable al caso concreto, pero indefectiblemente deberá ser de aplicación imperativa e inmediata, en aras de la protección de los derechos de la infancia[56].

Sin embargo, en el caso específico de los menores, la preocupación por tener una protección mayor de sus derechos a la protección de datos personales ha ido incrementándose por parte de los Estados, teniendo en cuenta el papel que sus padres o cualquier otra persona que tenga bajo su responsabilidad el cuidado de los mismos en la formación personal de ellos, que incluye el uso responsable y seguro de sus datos personales en internet y las redes sociales que se usan a través del ciberespacio.

Los menores de edad, sus padres, tutores, hermanos, otros familiares, amigos y cualquier otra persona comparten información (videos e imágenes) relativa a los datos personales de los primeros, son personajes que exponen a los niños en las redes sociales.

En este punto, es necesario citar la sentencia T-260/12 emitida por la Sala Octava de Revisión de la Corte Constitucional de la República de Colombia del 29

---

[55] González Martín, Nuria y Rodríguez Benot, Andrés, (coords.), "Adopción Internacional", *Estudios sobre adopción internacional*, UNAM, Instituto de Investigaciones Jurídicas, México, 2001, p.38.

[56] Cárdenas Miranda, Elva L, "El interés superior del niño", *Revista Letras Jurídicas*, México, 2011, Vol. 23, julio-diciembre 2010, p.6, *http://letrasjuridicas.com.mx/Volumenes/23/18a.pdf*.

de marzo de 2012[57], en la que una señora solicitó la protección de los derechos fundamentales de su hija de 4 años, ya que los consideró vulnerados con la creación de una cuenta en la red social Facebook por parte del padre de la menor.

Por su lado, el señor manifestó que creó tal cuenta con el fin de mantener el contacto con su hija, ya que, debido a problemas con la madre, transcurren largas temporadas sin que pueda ver a la niña; para la creación del perfil de la menor, el padre mintió sobre la edad de ésta, pues en ese momento ella tenía la edad de 4 años y las reglas de la red social Facebook indican que es necesario tener 13 para poder acceder a la misma.

También manifestó realizó una adecuada configuración de privacidad, al aceptar como amigos sólo a aquellas personas que tenían un parentesco o relación cercana con la menor, por lo que la Sala de Revisión determinaría si se vulneran los derechos fundamentales al habeas data[58], la honra y el interés superior de la menor, con la creación de una cuenta en Facebook.

De esta manera, la Sala precisó que "si bien la patria potestad implica la posibilidad de que los padres tomen ciertas decisiones en nombre de sus hijos, como sería en este caso, la creación de una cuenta en red social, tales decisiones no pueden poner en riesgo a los mismos, ni afectar sus derechos fundamentales, como sucede en este caso".

Por tanto, y con el fin de tutelar los derechos fundamentales de la niña al habeas data y a la honra, así como el interés superior de la menor, se ordenó la

---

[57] Corte Constitucional de la República de Colombia, Sentencia T-260/12 emitida por la Sala Octava de Revisión, 29 de marzo de 2012, *http://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM.*

[58] De acuerdo con Muñoz de Alba, Habeas Data es un "recurso procesal diseñado para controlar la información personal contenida en bancos de datos, cuyo derecho implica la protección, la cancelación, y la posibilidad de restringir y limitar la circulación de los mismos." Muñoz de Alba Medrano, Marcia, *Habeas Data*, México, UNAM, Instituto de Investigaciones Jurídicas, 2006, p. 2, *http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf*.

cancelación de la cuenta en Facebook a nombre de la niña por parte de su padre, se advirtió de no crear una cuenta en cualquier red social análoga a Facebook, con datos personales y sensibles de la menor.

En este caso es posible observar el deber del Estado de proteger los derechos fundamentales de la menor, en el contexto de la creación de una cuenta en una red social de la que ella no cuenta con el criterio necesario para su uso y menos para compartir sus datos personales; de igual manera sirve este precedente como mecanismo para no se les prohíba a los menores el acceso a la Sociedad del Conocimiento y la Tecnología, atendiendo entre otras cosas a las recomendaciones del Memorándum de Montevideo (las cuales se analizarán más adelante), en lo referente a que tal acceso debe ser paulatino, acompañado de las personas encargadas de su cuidado y acorde a la madurez y desarrollo psicológico que presenten.

Capítulo 2

Antecedentes, marco jurídico de la protección de datos personales

Capítulo 2: Antecedentes, marco jurídico de la protección de datos personales

2.1. Antecedentes del derecho de protección de datos personales y a protección de datos personales desde las distintas familias jurídicas

El Derecho a la Protección de Datos Personales, en adelante DPDP, es definido por Pulido como "la protección jurídica con la que cuentan las personas respecto a la recopilación, almacenamiento, utilización, transmisión y cualquier otra operación realizada sobre cierta información personal con características particulares a la que se le han llamado datos personales"[59]. De esta manera la protección de este derecho se refiere a toda información personal por la naturaleza de la misma.

Además, el mencionado Derecho Fundamental, cobra una mayor injerencia en el actuar de cualquier ente privado o gubernamental debido a la evolución normativa que se ha desarrollado a partir de diversos hechos que involucran el uso de datos personales y que dan origen a múltiples componentes del DPDP.

Antes de indicar la evolución de este Derecho, no sobra indicar que conforme al Derecho Anglosajón la existencia del *Privacy* tuvo un origen eminentemente jurisprudencial, a partir del ensayo elaborado por Warren y Brandeis cuyo contenido está encaminado a detener cualquier tipo de intromisión en la vida privada de las personas, especialmente por parte de la prensa[60]. Esta referencia, fungió como

---

[59] Pulido Jiménez, Miguel, "Convergencias y divergencias: Acceso a la Información y la tutela de los datos personales", *Retos de la protección de dato personales en el sector público*. México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011, p. 89, *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf*

[60] Este primer acercamiento, resultó ser la formulación teórica hasta su reconocimiento jurisdiccional en Estados Unidos e incluso su aparición como Derecho Fundamental en el derecho continental o de la familia romano-germánica.

primer acercamiento a lo que hoy en día se entiende por privacidad y el origen de la autodeterminación informativa.

No obstante, en cuanto al DPDP en el Derecho Romano-Germánico o también conocido como Derecho Continental, desde la Declaración Universal de los Derechos Humanos de 1948 y en la Convención para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950, se estableció un primer acercamiento a la protección de la vida privada en sus artículos 12, así como 8 y 10 respectivamente[61].

El Dr. Carlos G. Gregorio también identifica la evolución del DPDP en Europa derivado del origen que tuvo a partir del fin de la Segunda Guerra Mundial, así como de las múltiples normas nacionales aprobadas a lo largo de Europa, en las que es posible identificar en Alemania la Ley de Protección de datos (Datenschutz) de 1970, en la que se regulaba la protección de cualquier persona frente a la intromisión que el gobierno quisiera realizar en su vida privada[62].

Cabe señalar que, a finales de la década de los sesentas, el desarrollo de normativa en la materia fue en aumento, cada una con un origen sociológico distinto, pero con un mismo fin regular en el sector privado y público el tratamiento de datos personales previo consentimiento y autoridades que lo garanticen.

Warren, Samuel D. y Brandeis, Louis D, "The Right To Privacy", *Harvard Law Review*, Estados Unidos, 1890, Vol. IV, núm. 5, diciembre 1890, p. 206. *http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf*

[61] Gregorio, Carlos G., "Protección de datos personales: Europa vs Estados Unidos, todo un dilema para América Latina", en Hugo Cocha Cantú Hugo, Sergio López-Ayllón y Lucy Tacher Epelstein (coords.) *Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información*, México, UNAM, Instituto de Investigaciones Jurídicas, 2005, p. 307, *https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf*

[62] Ibídem, p. 308.

Por este motivo, surge el 28 de enero de 1981 en Estrasburgo, el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento de Datos de Carácter Personal, cuyo objeto consiste en "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos)"[63].

En este punto, es conveniente recordar que, derivado de la sentencia dictada por el Tribunal Constitucional de la República Federal Alemana en la sentencia sobre la Ley del Censo, de acuerdo con Martínez, se presentó el reconocimiento jurisprudencial de un Derecho Fundamental a la Autodeterminación Informativa, teniendo como idea primaria la facultad del individuo de decidir por sí mismo sobre la difusión y utilización de sus datos personales[64].

En el mismo orden de ideas, debido al comercio internacional y demás consecuencias de la globalización, resultó necesario emitir un documento que unificara las múltiples regulaciones en la materia, dando un paso enorme respecto del tratamiento de datos personales y a la libre circulación (transferencia) de los mismos, me refiero a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio de 1995, la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa además del tratamiento de los datos personales, a la protección de la intimidad en el sector de las telecomunicaciones,

---

[63] Disponible para su consulta en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf*

[64] Martínez, Ricard, "El derecho fundamental a la protección de datos: perspectivas", *Revista de Internet, Derecho y Política*, III Congreso Internet, Derecho y Política (IDP) Nuevas perspectivas, año 2007, núm. 5, p. 49, *https://dialnet.unirioja.es/descarga/articulo/2372613.pdf*

la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002 relativa a la protección de la intimidad en el sector de las comunicaciones electrónicas o directiva sobre la privacidad y las comunicaciones electrónicas y la Directiva 2006/ 24/CE sobre 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, teniendo como resultado la Carta Europea de Derechos Fundamentales en el que se incorpora el DPDP[65].

2.2. Marco jurídico internacional en materia de datos personales en redes sociales

A partir del desarrollo de las TIC, el mundo entero se ha envuelto en una serie de cambios interminables, en los que intervienen herramientas que son útiles para la sociedad desde el punto de vista de la libertad de expresión, el acceso a la información, el desarrollo de la integración social, entre otros elementos que se involucran por el uso que obtienen día a día.

De esta manera, dichas herramientas se vuelven mecanismos que sirven para el ejercicio de diversos derechos fundamentales de cualquier persona y derivado del mismo, aumenta la cantidad de beneficiados dentro de la diversidad social y cultural a nivel mundial.

Existen diversos instrumentos internacionales que contienen derechos de los menores, tales como la Convención sobre los Derechos del Niño, que dispone en su artículo 3, párrafo 1 que *"en todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño"*[66].

Como se ha mencionado a lo largo del presente documento, el interés superior del niño resulta ser un principio que debe prevalecer en todo momento que

---

[65] Ibídem, p. 50.

[66] Disponible para su consulta en *http://www.un.org/es/events/childrenday/pdf/derechos.pdf*

involucre el desarrollo del menor, por lo que no es exclusivo de autoridades, sino también de cualquier persona que conviva con este sector de la sociedad.

Si bien es complejo determinar cómo se debe de garantizar este principio, también lo es que a partir del respeto a la dignidad de cada ser humano y potencializar el ejercicio de sus derechos, probablemente se cumpla con lo establecido en este artículo de la Convención sobre los Derechos del Niño, iniciando por el interés superior del menor.

A su vez, en su artículo 3, párrafo 2, establece que *"los Estados partes se comprometen a asegurar al niño la protección y el cuidado que sean necesarios para su bienestar, teniendo en cuenta los derechos y deberes de sus padres, tutores u otras personas responsables de él ante la ley y, con ese fin, tomarán todas las medidas legislativas y administrativas adecuadas"*[67].

En este artículo se presenta una responsabilidad directa para el Estado, ya que tendrán el fin de proteger y cuidar a los menores de edad, respetando los derechos y deberes de los padres de familia, o cualquier persona responsable de ellos, adoptando las medidas necesarias para lograr su objetivo.

Sin embargo, desde esta perspectiva nos enfrentamos a una situación de hecho que supera al derecho, es decir el incumplimiento de las normas que emite el Estado para lograr la protección de este sector vulnerable.

A pesar de contar con normativa aplicable en nuestro país en materia de derechos de los niños, lamentablemente no se ha garantizado de manera plena para todos los menores de edad de México. Ejemplos de esto, se localiza con la gran cantidad de niños que sufren una mala alimentación, desnutrición, violencia, acceso a limitado a servicios de salud, pobreza, analfabetismo, discriminación, entre otros factores que impiden el desarrollo pleno de los niños, niñas y adolescentes[68].

---

[67] Ibídem.

[68] Esto puede comprobarse con las estadísticas que emitió el Instituto Nacional de Estadística y Geografía con motivo del Día del Niño (30 de abril) y del Día Internacional de la Niña (11 de octubre), disponibles para su consulta en *http://www.inegi.org.mx/saladeprensa/aproposito/2017/ni%C3%B1o2017_Nal.pdf* y

Tampoco se debe olvidar que el Principio 2 de la Declaración de las Naciones Unidas sobre los Derechos del Niño dispone entre otras cosas, que los niños gozarán "*de una protección especial y dispondrá de oportunidades y servicios, dispensado todo ello por la ley y por otros medios, para que pueda desarrollarse física, mental, moral, espiritual y socialmente en forma saludable y normal, así como en condiciones de libertad y dignidad. Al promulgar leyes con este fin, la consideración fundamental a que se atenderá será el interés superior del niño*"[69]

Este documento contiene diez principios correspondientes a la protección del niño, que conforme a su preámbulo van encaminados tanto antes como después del nacimiento, de tal manera que establece los derechos a la igualdad, a un nombre y nacionalidad, a la alimentación, a la educación, a recibir primero protección y socorro, entre otros.

Así, nos encontramos ante un documento que da pautas respecto del desarrollo integral del menor, reconoció la existencia de los derechos inherentes a los niños, y que a pesar del año en el que se aprobó (1959) siguen vigentes en la actualidad, por lo que, las autoridades deben tomar en cuenta al momento de adoptar las medidas pertinentes, el interés superior de los niños como su principal criterio de orientación.

A su vez, la Declaración Universal de Derechos Humanos de 1948, en su artículo 25, párrafo 2, establece que *"la maternidad y la infancia tienen derecho a cuidados de asistencia especiales"*, y que *"todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social"*[70].

---

http://www.inegi.org.mx/saladeprensa/aproposito/2017/Nina2017_Nal.pdf respectivamente.

[69] Disponible para su consulta en *https://www.oas.org/dil/esp/Declaraci%C3%B3n%20de%20los%20Derechos%20del%20Ni%C3%B1o%20Republica%20Dominicana.pdf*

[70] Disponible para su consulta en *http://www.un.org/es/universal-declaration-human-rights/*

Este documento resulta ser uno de los primeros documentos internacionales que incluyen en su texto la mención de los niños de manera expresa y que resulta el origen del reconocimiento de los derechos humanos internacionalmente, por ende, es el primer antecedente de los derechos de este sector de la sociedad.

En el mismo orden de ideas, el Pacto Internacional de Derechos Civiles y Políticos dispone en su artículo 24, párrafo 1 que *"todo niño tiene derecho, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, origen nacional o social, posición económica o nacimiento, a las medidas de protección que su condición de menor requiere, tanto por parte de su familia como de la sociedad y del Estado"*[71].

Es decir, con este Instrumento Internacional, los Estados partes deben garantizar múltiples libertades de las personas sin su intervención, de manera que se involucre el ejercicio de derechos propios de la ciudadanía y del individuo en sí mismo, sin que participe el Estado en sus límites. Respecto de lo menores de edad, exige que el Estado, su familia y el Estado, los proteja por medio de las medidas necesarias y sin estar sujetos a cualquier tipo de discriminación.

De igual forma, el Pacto Internacional de Derechos Económicos, Sociales y Culturales, en su artículo 10, párrafo 3 establece como deber de los Estados parte "*adoptar medidas especiales de protección y asistencia en favor de todos los niños y adolescentes, sin discriminación alguna por razón de filiación o cualquier otra condición. Debe protegerse a los niños y adolescentes contra la explotación económica y social. Su empleo en trabajos nocivos para su moral y salud, o en los cuales peligre su vida o se corra el riesgo de perjudicar su desarrollo normal, será sancionado por la ley. Los Estados deben establecer también límites de edad por debajo de los cuales quede prohibido y sancionado por la ley el empleo a sueldo de mano de obra infantil*."[72]

---

[71] Disponibles para su consulta en *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx*

[72] Disponible para su consulta en *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx*

Este instrumento internacional junto con el Pacto Internacional de Derechos Civiles y Políticos, devienen de la Declaración Universal de los Derechos Humanos, por lo que, en este caso el Estado debe intervenir a través de las medidas que correspondan en la garantía de los derechos que en él se encuentran establecidos, tales como el nivel de vida adecuado, a la buena salud, educación, trabajo y derechos culturales. Respecto de los niños, la participación del Estado implica protegerlos entre otras cosas, de explotación económica y social hecha por cualquier persona, así como de su empleo en trabajos nocivos para su moral y salud.

A su vez el artículo 19 de la Convención Americana de Derechos Humanos, dispone que *"todo niño tiene derecho a las medidas de protección que su condición de menor requiere por parte de su familia, de la sociedad y del Estado"*[73].

Motivo por el cual, se reitera que los menores de edad requieren de una protección mayor por parte de todas las personas que convivan con ellos, desde su círculo más cercano en la familia, su desarrollo en la sociedad y a través del ejercicio de sus derechos, garantizados en todo momento por el Estado.

Con los instrumentos internacionales ya identificados, tanto los estados como la sociedad en general, deben llevar a cabo diversos cambios en su normativa, que inicien con la atención de acciones frente a los menores que procuren en todo momento el bienestar de este sector de la sociedad.

Por otro lado, en cuanto a la vida privada de las personas; una primera aproximación de protección en la esfera íntima de la persona se encuentra enunciada en el ámbito internacional dentro de la Declaración Universal de los Derechos Humanos de 1948, cuyo artículo 12 señala: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques[74]".

---

[73] Disponible para su consulta en *https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm*

[74] Disponible para su consulta en *http://www.un.org/es/documents/udhr/*

Dicha enunciación, considerada como el derecho a la intimidad en su ámbito estático, se encuentra reconocida en la mayoría de las normas constitucionales, sin olvidar que, en cuanto a la intimidad en su ámbito abierto y derivado del desarrollo tecnológico, pueden ser vulnerados otros aspectos de la esfera íntima de la persona, como lo pueden ser sus datos personales.

Sin embargo, en el caso específico de los menores, la preocupación por tener una protección mayor de sus datos personales ha ido incrementándose por parte de los Estados teniendo en cuenta el papel que sus padres o cualquier otra persona que tenga bajo su responsabilidad el cuidado, pero evidentemente de los mismos en la formación personal de ellos, que incluye en las redes sociales, quienes buscan que se incluya la cultura y promoción del uso responsable y seguro de sus datos personales en internet, específicamente en las redes sociales que se usan a través del ciberespacio.

Debido a la importancia del tema, es necesario partir del instrumento internacional que, por excelencia, reconoce la responsabilidad del Estado e incluso de la sociedad, de la protección de los infantes y adolescentes, esto es la Convención sobre los Derechos del Niño[75].

En dicho instrumento internacional se reconoce entre otras cosas, la responsabilidad que existe respectivamente por parte de la sociedad y el Estado, en la protección de los menores, a partir del papel relevante que cumple la familia, o quien se encuentre del cuidado de los mismos en el proceso de educación sobre el uso responsable y seguro de herramientas como Internet y las redes sociales digitales y en la protección y garantía de sus derechos; la necesidad de priorizar en todo momento el interés superior de las niñas, niños y adolescentes, guardando un equilibrio entre las necesidades de protección contra la vulneración de sus derechos y el uso responsable de esas herramientas, así como el ejercicio de otros derechos como el acceso a la información, la libertad de expresión, entre otros.

---

[75] Disponible para su consulta en *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx.*

Por lo que se busca que todo aquel que se beneficie de cualquier forma de Internet y por el uso de la información que se recaba a través de las redes sociales digitales, a su vez, sean responsables por los servicios que proveen y por tanto deben asumir su responsabilidad en las soluciones a la problemática que se genera[76], frente a la probable vulneración a los titulares de los datos personales que recaban.

Por este motivo, el 28 de julio de 2009 en Montevideo, Uruguay, se elaboró el *Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes*[77], el cual estableció entre otras cosas, que el Estado debe proveer información y fortalecer capacidades de los padres, sobre los eventuales riesgos a que se enfrentan los menores en internet.

Sin que lo anterior implique que se debe dejar de 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 permita obtener los mismos resultados, sin ser restrictiva de derechos.

En el memorándum indicado, se especifica que se debe transmitir claramente a las niñas, niños y adolescentes que internet no es un espacio sin normas, impune o sin responsabilidad, por lo que la participación anónima o el uso de pseudónimos, debe involucrar el respeto a la privacidad, intimidad y buen nombre de terceras personas, responsabilidades civiles, penales y administrativas que se existen cuando se vulneran derechos propios o de terceros en la red, entre otros aspectos.

Además, se especifica que la educación sobre la sociedad de la información y el conocimiento, en especial para el uso responsable y seguro de Internet, incluyendo las redes sociales digitales, con el fin de evitar las potencialidades y riesgos, así como la capacitación correspondiente en el tema.

---

[76] Artículos 2, 3, 5, 12, 13, 29, 34 de la Convención sobre los Derechos del Niño.

[77] Disponible para su consulta en *http://www.iijusticia.org/Memo.htm*

Es necesario recalcar que, si bien este documento abarca un gran número de recomendaciones en materia de prevención y educación, para los Estados sobre el marco legal, para la aplicación de las leyes, en materia de políticas públicas y para la industria, debido a su origen, no resulta ser un instrumento vinculante para los Estados que forman parte de él.

Primero por el procedimiento en el que fue elaborado, que no cumple con las características de un tratado internacional, toda vez que se emitió como un documento de trabajo del Seminario Derechos, Adolescentes y Redes Sociales en Internet, realizado en Montevideo los días 27 y 28 de julio de 2009, integrado por representantes de instituciones públicas y privadas de diversos países; y segundo, porque el fin del Memorándum no era la emisión de un marco jurídico aplicable, sino que los diversos actores involucrados "se comprometan con el tema para extender los aspectos positivos de la Sociedad de la Información y Conocimiento, incluyendo Internet y las redes sociales digitales, así como prevenir aquellas prácticas perjudiciales que serán muy difíciles de revertir, así como los impactos negativos que las mismas conllevan"[78]

Así las cosas, el Memorándum de Montevideo surge como respuesta a "la realidad social, cultural y jurídica de la región iberoamericana"[79] en el marco de la era digital y la protección de datos personales, por lo que hasta la fecha sirve como

[78] Lo anterior, conforme a las consideraciones generales del Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en internet, en particular de niños, niñas y adolescentes, disponible para su consulta en *http://www.iijusticia.org/Memo.htm*

[79] Bernier, Chantal. "El Memorándum de Montevideo: un marco de referencia para la protección de los datos personales de los jóvenes en Internet en la región Iberoamericana", en Gregorio, Carlos G. y Ornelas Lina (comps.) *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes*, Instituto de Investigación para la Justicia e Instituto Federal de Acceso a la Información y Protección de Datos, México, 2011, p. 17, *http://libros.metabiblioteca.org/bitstream/001/307/9/978-968-5954-59-4.pdf*

guía de actuación de los sujetos responsables de la privacidad de niños en Internet, incluyendo las redes sociales.

En el mismo orden de ideas, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), publicado el 4 de mayo en el Diario Oficial de la Unión Europea, establece diversas obligaciones y derechos relativos a la protección de datos personales dentro del territorio de la Unión Europea, así como para cualquier responsable que, incluso fuera de ella en virtud del Derecho Internacional Público.

Cabe señalar que este Reglamento contiene múltiples cambios en la normativa relativa a la protección de datos personales, por lo que su ámbito de aplicación se extiende a todos los países miembros de la Unión Europea y se aplicará directamente en todos ellos a partir del 25 de mayo de 2018, fecha en la que deberán de ajustar todos los responsables, los cambios correspondientes a su normativa y al tratamiento de datos personales que realizan para su cumplimiento.

Ahora bien, para efectos del presente trabajo, se referirá a lo previsto en el artículo 8 del mencionado Reglamento, relativo a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.

Dicho artículo establece que en relación con la oferta directa a niños de servicios de la sociedad de la información, como es el uso de redes sociales en Internet, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años, por el contrario si es menor a esa edad el tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó[80].

[80] Disponible para su consulta en: *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europe*

Asimismo, prevé que los Estados miembros puedan establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

En la interpretación del mencionado artículo, es posible decir que los niños, niñas y adolescentes se encuentran dentro del ámbito de protección del Reglamento Europeo, sin importar su edad, pero siempre y cuando se verifique que se cumplan los principios relacionados con el tratamiento de datos personales, por parte de cualquier responsable dentro de la Unión Europea, con las modalidades establecidas en él.

2.3. Marco jurídico nacional en materia de datos personales en redes sociales y derecho de los niños, niñas y adolescentes

México a lo largo de las últimas décadas ha logrado fomentar la protección, por un lado, de diversos bienes jurídicos y más importante aún, de derechos humanos, a partir de diversas reformas a su Constitución impulsadas por la suscripción de diversos Tratados Internacionales, las determinaciones de Organismos Internacionales como la Corte Interamericana de Derechos Humanos e incluso interpretaciones bajo el principio pro persona de parte de sus tribunales.

Otro de los cambios que México realizó en los últimos años se reflejó en diversas reformas constitucionales enfocadas a la adecuación de su legislación frente a los múltiples tratados internacionales que adoptó.

Una de las principales, es la reforma de abril del 2000 al artículo 4° Constitucional, que reconoce que los niños y niñas[81] son titulares del derecho a la

---

a/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf

[81] No resulta óbice hacer referencia a reformas Constitucionales anteriores respecto a los derechos de los menores de edad, tales como la publicada el 18 de marzo de 1980 al mismo Artículo 4°, dando origen al deber de los padres de preservar el derecho de los primeros a la satisfacción de sus necesidades y a su salud física y mental; sin embargo, para efectos del presente trabajo, se enfocará al estudio de

satisfacción de sus necesidades de alimentación, salud, educación y sano esparcimiento para su desarrollo, y estableciendo que los ascendientes, tutores y custodios tienen el deber de preservar estos derechos, mientras el Estado es responsable de proveer lo necesario para propiciar el respeto a la dignidad de la niñez y el ejercicio pleno de sus derechos y otorgar facilidades a los particulares para que coadyuven al cumplimiento de los derechos de la niñez[82].

El mismo artículo fue reformado el 12 de octubre de 2011, cuyo cambio consistió en la inclusión dentro del marco jurídico mexicano y en específico, en todo el actuar del Estado, del deber de cumplir con el principio del interés superior de la niñez, con el fin de garantizarles de manera plena sus derechos, incluyéndose en el diseño, ejecución, seguimiento y evaluación de las políticas públicas dirigidas a la niñez[83].

Por otro lado, en cuanto a partir de la reforma al Artículo 6º de la Constitución Política de los Estados Unidos Mexicanos del 20 de Julio de 2007 se incorporó la protección a los datos personales (hasta ese entonces como garantía individual) como una limitante al derecho de acceso a la información, de la siguiente manera "II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá

---

las más relevantes para el estudio de la protección de los niños, niñas y adolescentes en el marco jurídico mexicano.

[82] Disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_148_07abr00_ima.pdf*

[83] Además, estableció la obligación a los ascendientes, tutores y custodios de los niños y niñas, de preservar y exigir el cumplimiento de este principio y demás derechos de la niñez. Disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_198_12oct11.pdf*

acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos”[84].

Así las cosas, el 1° de junio de 2009 la Reforma Constitucional del Artículo 16 estableció de manera expresa el DPDP de la siguiente manera “Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros”[85].

Asimismo, resulta fundamental mencionar que el pasado 10 de junio de 2011, se reformó nuevamente la Constitución Política de los Estados Unidos Mexicanos, misma que tuvo como efecto, un cambio paradigmático en el orden jurídico nacional, así como en la administración de justicia federal.

Dicha reforma trajo consigo el reconocimiento de la progresividad de los derechos humanos, mediante la expresión clara del principio pro persona como rector de la interpretación y aplicación de las normas jurídicas, en aquellas que favorezcan y brinden mayor protección a las personas, lo cual trajo como consecuencia la obligación expresa de observar los tratados internacionales firmados por el Estado mexicano, que a la postre, tiende al mejoramiento de las condiciones de vida de la sociedad y al desarrollo de cada persona en lo individual.

Es decir, frente al choque de derechos que se genera en una situación determinada, la autoridad debe constatar primero la vulneración o no aplicación de un derecho fundamental frente a otro, que a su vez sea trascendental dicha inobservancia para que finalmente se determine si ésta resulta ser adecuada por el incumplimiento o no aplicación del segundo derecho que resultó tener un ejercicio nugatorio.

---

[84] Reforma disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_174_20jul07_ima.pdf*

[85] Reforma disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf*

En este sentido, el Poder Judicial Federal de México, reiteró la validez de las sentencias emitidas por la Corte Interamericana de Derechos Humanos y reconoció la vigencia de los tratados internacionales dentro del ordenamiento jurídico interno, generando por consecuencia la obligación de las autoridades nacionales de aplicar los derechos humanos de conformidad con la Constitución y los tratados internacionales vigentes en nuestro país. Lo anterior se encuentra sustenta en la tesis que se muestra a continuación para pronta referencia:

CORTE INTERAMERICANA DE DERECHOS HUMANOS. EFECTOS DE SUS SENTENCIAS EN EL ORDENAMIENTO JURÍDICO MEXICANO. El Estado Mexicano se adhirió a la Convención Americana sobre Derechos Humanos el 24 de marzo de 1981 y reconoció la competencia contenciosa de la Corte Interamericana de Derechos Humanos el 16 de diciembre de 1998, mediante declaración unilateral de voluntad que fue publicada en el Diario Oficial de la Federación el 24 de febrero de 1999. En ese sentido, los artículos 133 y 1o. de la Constitución Política de los Estados Unidos Mexicanos reconocen la vigencia de los tratados internacionales en nuestro ordenamiento jurídico interno y establecen la obligación de las autoridades nacionales de aplicar los derechos humanos de conformidad con la Constitución y los tratados internacionales vigentes en nuestro país. Por lo anterior, la ratificación de la Convención Americana sobre Derechos Humanos y el reconocimiento de la jurisdicción contenciosa de la Corte Interamericana de Derechos Humanos, generan como una consecuencia ineludible que las sentencias emitidas por dicho tribunal internacional, en aquellos casos en los cuales México haya sido parte en el juicio, resulten obligatorias para el Estado mexicano, incluidos todos los jueces y tribunales que lleven a cabo funciones materialmente jurisdiccionales. Esta obligatoriedad alcanza no sólo a los puntos resolutivos de las sentencias en comento, sino a todos los criterios interpretativos contenidos en las mismas[86].

Ahora bien, un elemento fundamental respecto de la interpretación normativa con base en la teoría de la ponderación, resulta ser el principio pro persona (pro

[86] Tesis. 1a. XIII/2012, Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro V, febrero de 2012, Pág. 650.

homine), mismo que dada la complejidad que amerita poder desagregar los diversos elementos que lo componen, la Suprema Corte de Justicia de la Nación emitió la siguiente tesis, que resulta ser clara en cuanto al ejercicio de la ponderación de derechos en las que se invoque este principio, y que da la pauta para permitir la aplicación de los diversos tratados internacionales de derechos humanos que se indicaron líneas arriba, dentro del sistema jurídico mexicano:

PRINCIPIO PRO HOMINE. VARIANTES QUE LO COMPONEN. Conforme al artículo 1o., segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, las normas en materia de derechos humanos se interpretarán de conformidad con la propia Constitución y con los tratados internacionales de la materia, procurando favorecer en todo tiempo a las personas con la protección más amplia. En este párrafo se recoge el principio "pro homine", el cual consiste en ponderar el peso de los derechos humanos, a efecto de estar siempre a favor del hombre, lo que implica que debe acudirse a la norma más amplia o a la interpretación más extensiva cuando se trate de derechos protegidos y, por el contrario, a la norma o a la interpretación más restringida, cuando se trate de establecer límites a su ejercicio. En este contexto, desde el campo doctrinal se ha considerado que el referido principio "pro homine" tiene dos variantes: a) Directriz de preferencia interpretativa, por la cual se ha de buscar la interpretación que optimice más un derecho constitucional. Esta variante, a su vez, se compone de: a.1.) Principio favor libertatis, que postula la necesidad de entender al precepto normativo en el sentido más propicio a la libertad en juicio, e incluye una doble vertiente: i) las limitaciones que mediante ley se establezcan a los derechos humanos no deberán ser interpretadas extensivamente, sino de modo restrictivo; y, ii) debe interpretarse la norma de la manera que optimice su ejercicio; a.2.) Principio de protección a víctimas o principio favor debilis; referente a que en la interpretación de situaciones que comprometen derechos en conflicto, es menester considerar especialmente a la parte situada en inferioridad de condiciones, cuando las partes no se encuentran en un plano de igualdad; y, b) Directriz de preferencia de normas,

la cual prevé que el Juez aplicará la norma más favorable a la persona, con independencia de la jerarquía formal de aquélla[87].

Por otro lado, retomando el derecho a la protección de los derechos de los niños, niñas y adolescentes, el 4 de diciembre de 2014 se publicó en el Diario Oficial de la Federación la Ley General de los Derechos de Niñas, Niños y Adolescentes[88], instrumento normativo que conforme a su artículo 1° tiene por objeto, entre otras cosas, reconocer a niñas, niños y adolescentes como titulares de derechos; garantizar el pleno ejercicio, respeto, protección y promoción de sus derechos humanos conforme a lo establecido en la Constitución Política de los Estados Unidos Mexicanos y en los tratados internacionales de los que el Estado mexicano forma parte; y establecer las bases generales para la participación de los sectores privado y social en las acciones tendentes a garantizar la protección y el ejercicio de sus derechos, así como a prevenir su vulneración.

Resulta de toral importancia indicar que con la Ley General referida, se crean diversas instituciones e instruye a las demás autoridades de los tres niveles de gobierno (federal, estatal y municipal), que garanticen la protección de los derechos de niñas, niños y adolescentes a través de un enfoque integral, transversal y con perspectiva de derechos humanos, conforme a los principios rectores que en ella se establecen, como lo son el interés superior de la niñez (de manera primordial) y el principio pro persona, entre otros[89].

En cuanto a la protección de datos personales en México, se debe diferenciar entre la regulación aplicable tanto al sector público como al privado. Respecto del

---

[87] Tesis I.4o.A.20 K Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 1, diciembre de 2013, pág. 1211.

[88] Con esta Ley, se abrogó la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, de aplicación y alcance mucho menor en cuanto a la protección de los derechos de este sector de la sociedad. Disponible para su consulta en: *http://www.dof.gob.mx/nota_detalle.php?codigo=5374143&fecha=04/12/2014*

[89] Artículos 2 y 6 de la Ley General de los Derechos de Niñas, Niños y Adolescentes.

sector público, resulta aplicable la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)[90], con la que se pretende garantizar el ejercicio del derecho fundamental a la protección de datos personales, ampliando su ámbito de aplicación, siendo de observancia general en toda la República Mexicana.

De acuerdo con el artículo 1° de dicha Ley, tiene por objeto "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados", entendiendo por estos a todo ente del ámbito federal, estatal y municipal, y cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

En ese sentido, cualquier persona tiene el derecho de ejercer sus derechos ARCO (acceso, rectificación, corrección y oposición) ante los sujetos obligados de la LGPDPPSO, cuyo principal objetivo es garantizar el ejercicio de este Derecho Fundamental.

Los derechos ARCO pueden ser ejercidos en todo momento por el titular o su representante, y para el caso de menores de edad se ejercerá de conformidad con las leyes civiles, respecto de las reglas de representación dispuestas en la misma legislación[91].

Siguiendo con el marco normativo nacional en materia de protección de datos personales, México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP). Esta norma se publicó en el Diario

---

[90] Publicada en el Diario Oficial de la Federación el 26 de enero de 2017. Disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*

[91] En concatenación con lo ya mencionado respecto del Interés Superior de la Niñez, cada autoridad tiene el deber de preservar el mejor desarrollo de los niños, niñas y adolescentes, incluyendo el ejercicio de sus derechos, conforme a la normativa nacional y los tratados internacionales de los que México forma parte, actuando para tales efectos de manera transversal, en el ámbito de sus atribuciones.

Oficial de la Federación el 5 de julio de 2010[92] y tiene por objeto, conforme a su artículo 1° "regular su tratamiento (de los datos personales) legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas".

En primer instancia esta Ley Federal permite a cualquier persona física ejercer sus derechos ARCO ante cualquier particular que lleve a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Cabe señalar que ambas leyes de protección de datos personales, el principal ente protector de este Derecho Fundamental es el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual cuenta con diversas atribuciones para garantizar el DPDP en México.

Aunado a la LFPDPPP, también debe hacerse especial mención a su Reglamento, publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011. Este instrumento normativo tiene por objeto reglamentar las disposiciones de dicha Ley Federal, lo cual permite establecer de manera más específica su ámbito de aplicación, los principios y deberes rectores de la protección de datos personales y los procedimientos correspondientes al ejercicio de derechos ARCO, verificación y de imposición de sancionas, sin olvidar los esquemas de autorregulación que incluyó en el marco jurídico mexicano de la protección de datos personales en el sector privado, entre otros temas.

En este punto, resulta necesario reiterar lo antes mencionado respecto de lo establecido en su artículo 89, consistente en la limitación que tienen los menores de edad para el ejercicio de sus derechos ARCO, ya que deberán de llevarlos a cabo conforme a las reglas de representación dispuestas en el Código Civil Federal, pero

---

[92] Disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*

no se establece una limitante para el otorgamiento de su consentimiento en el tratamiento de sus datos personales, por lo que existe la presunción de un consentimiento viciado, cuando sea otorgado por una persona distinta al menor (titular de los datos personales), conforme a los artículos 11 a 21 de dicho Reglamento.

Así, en el sistema jurídico de México coexisten leyes para la protección de los derechos de niños en materia civil, penal y laboral, así como la protección de sus datos personales, sin olvidar las leyes en materia de salud; educación y cualquier otra vinculada con su desarrollo social, en las que invariablemente se invoca la protección al interés superior de la niñez.

2.4. Problemas para proteger los datos personales en redes sociales desde una concepción tradicional

Si bien la mayoría de normativa aplicable a nivel mundial establece que los datos recolectados deben utilizarse únicamente para la finalidad expresamente señalada (principio de finalidad), también establece diversos mecanismos de acceso por parte de los titulares de esos datos (derecho de Acceso) de los cuales siempre debe de estar informado por parte del responsable.

Por este tipo de conductas, en las que cada vez se envía más información como fotos, videos, comentarios, cookies, búsquedas de páginas o diversas conductas dentro de las redes sociales, el uso y disposición de esos datos constituye un valor comercial, sin que los titulares conozcan el derecho de proteger dichos datos personales.

De acuerdo con la empresa Symantec[93], “los delincuentes de Internet utilizan el mercado clandestino para comprar y vender bienes y servicios ilegales, como datos robados, cuentas comprometidas en línea, malware personalizado, servicios e infraestructura de ataque, cupones fraudulentos y mucho más. De esta manera, los precios de los bienes y servicios ilegales llegan a variar ampliamente

[93] Disponible para su consulta en *http://www.symantec.com/connect/blogs/cuanto-cuestan-los-datos-robados-y-servicios-de-ataque-en-el-mercado-clandestino*

dependiendo de lo que se ofrece, pero pueden satisfacer a los ciberdelincuentes que tengan poco presupuesto, ya que, por ejemplo, se pueden obtener datos robados y cuentas comprometidas por menos de un dólar."

Por lo anterior, es probable que la información que se recaba, que contiene entre otras cosas una gran cantidad de datos personales podría variar en cuanto al valor que en el mercado negro podría llegar a adquirir entre los diversos hackers, ciberdelincuentes o peor aún en la Deep web[94], siendo así que una base de datos con información sensible de usuarios de redes sociales, sea objeto de diversas subastas con tal de poder disponer de los datos personales de una infinidad de usuarios.

En la actualidad, formamos parte de plataformas de intercambio de información y datos. Si existe la posibilidad de acceder a una mayor cantidad de datos disponibles, las redes sociales los han multiplicado y la tendencia internacional marca que esto se incrementará en los próximos años.

Por ello, debemos tener conciencia de la existencia del marco legal para nuestra protección, sobre todo, ser conscientes del uso y destino que les damos a

---

[94] Deep Web o también llamada "web oculta -la internet oculta- es la parte de internet a cuya información no es posible acceder de manera total mediante los buscadores, porque no es posible indexar las páginas de los sitios. Lo anterior debido a que el acceso, a las mismas, se encuentra restringido, ya sea por contraseña -como ocurre con los correos electrónico o sistema de bases de datos en línea de las empresas o de instituciones de gobierno- o mediante el llenado de un formulario que le permite al usuario solicita información para acceder a ésta; sirva de ejemplo, para este último caso, las bibliotecas virtuales y los formularios de páginas de comercio electrónico." Amaro López, José Antonio, Chávez Aceves, Ch. y Varela Navarro, Gerardo Alberto, "La Web Oculta y cómo los buscadores encuentran la información", *Paakat: Revista de Tecnología y Sociedad*, año IV, núm. 7, septiembre 2014 - febrero 2015, *http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/221/326#referencias*

nuestros datos (fotos, videos, información sobre nuestra vida, gustos, salidas, vacaciones, etc.). Debemos recordar que son elementos que configuran el ámbito íntimo de nuestra persona, y por todo esto debemos cuidarlos, sobre todo los de menores de edad.

En la exposición dentro de Internet, se generan situaciones de riesgo por compartir los datos personales al momento de utilizar las TIC como principal medio para hacer y mantener relaciones personales e incluso agregar personas desconocidas en la red de contactos, así como generar actos jurídicos, principalmente mercantiles.

Un ejemplo claro de la preocupación que existe por el valor que pueden llegar a tener los datos personales, se localiza en la sentencia recién emitida del Tribunal de Justicia de la Unión Europea el pasado 6 de octubre del 2015, en la que se determinó la invalidez de la Decisión 2000/520/CE de la Comisión Europea, del 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada[95] y solicita a la Comisión que invalide la norma según la cual el territorio era considerado seguro para la intimidad de los ciudadanos europeos desde hace 15 años.

Lo anterior, afecta directamente al acuerdo *safe harbour*[96] ya que hay más de 4,400 empresas que dependen de este acuerdo ya que tendrán que reestructurar

---

[95] Véase la sentencia en el siguiente vínculo electrónico: Sentencia del Tribunal de Justicia (Gran Sala) de 6 de octubre de 2015, C-362/14, *http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES*

[96] Puerto seguro: Se trata de un pacto entre Estados Unidos y la Comisión Europea que, hasta el momento, permitía a las empresas transferir datos a través del Atlántico. La condición que la UE ponía para esa transferencia era que se realizara con países que respetasen el marco legal europeo de protección de la privacidad, como, por ejemplo, notificar al cliente cuando se utilizan informaciones personales y con qué finalidades. El País, *¿Qué dice la sentencia del Tribunal de la UE sobre protección de datos?*, Madrid, 6 de octubre de 2015,

su línea de negocios para evitar una infracción de la normativa comunitaria, aunado a que con el nivel de globalización que existe hoy en día, las empresas más pequeñas son las que más sufrirán la interrupción de este pacto en Europa y las más grandes seguramente encontrarán la manera en la que se puede seguir llevando a cabo la transferencia de datos personales.

A partir de la observación realizada de las prácticas más comunes en redes sociales, un escenario peculiar, lo identifico por medio de la normativa aplicable a la protección de datos personales de menores, no sólo en México, sino en otros países, además de la relativa a la regulación de las redes sociales.

Si bien es claro que el hecho de regular cualquier actividad o conducta de la sociedad, no implica que pueda afectar o inhibir el desarrollo de la actividad regulada, también lo es que se ha elaborado a nivel mundial una gran cantidad de normativa relacionada con la protección de datos personales y ordenamientos que pretenden regular los contenidos que se pueden publicar en redes sociales a través de Internet.

Tal es el caso de España, Argentina y Francia por mencionar algunos ejemplos en los que se busca legislar lo relativo a las redes sociales y en algunos aspectos los datos personales de los usuarios.

En relación, con lo anterior las autoridades encargadas de regular la protección de datos personales, en México sería entre otras, el Instituto Nacional de Acceso a la Información y Protección de Datos Personales (INAI), que mientras fue el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), emitió muy pocas determinaciones en materia de protección de datos dentro de redes sociales[97].

---

http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444134525_731477.html

[97] Cabe señalar que el pasado 10 de abril de 2017, el INAI emitió algunas recomendaciones para usuarios de redes sociales, consistentes en 7 medidas preventivas de datos personales en las redes sociales y acciones encaminadas al uso responsable de los mismos, las cuales están disponibles en

2.4.1. Múltiples actores, jurisdicciones y conflictos de competencia de autoridades locales en materia de protección de datos personales

Ante los múltiples problemas que podrían presentarse en la red de redes, existen diversos entes que son responsables de garantizar, en el ámbito de su competencia, del Derecho a la Protección de Datos Personales.

Por un lado, autoridades y organismos públicos que traten datos personales en el ejercicio de sus atribuciones, tienen el deber de cumplir con toda la normativa relacionada con este Derecho Fundamental, respetando en todo momento la suma de principios y derechos de protección de dato personales. Al formar parte del Estado, es necesario reiterar el deber de cuidado con el que cuentan este tipo de Instituciones, y que en México están reguladas por la LGPDPPSO, por cuanto hace al sector público.

En cambio, dentro del sector privado se encuentran todas las personas físicas o jurídicas, que realizan tratamiento de datos personales y si bien podría inferirse que no cuentan con una obligación de proteger esta clase de información, lo cierto es que, en diversos casos, se ha mostrado que cuentas con estándares

---

http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-089-17.pdf y que fueron retomadas el 16 de mayo y 28 de julio, ambos de 2017, con enfoque hacia la seguridad para usuarios de redes sociales y la información que comparten en las mismas, disponibles en: *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-136-17.pdf* y *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-235-17.pdf* . Asimismo, el 13 de abril el INAI, a través de su Secretaría de Protección de Datos Personales, emitió 9 sugerencias relacionadas con la sincronización de datos personales en aplicaciones con los que se utilizan en redes sociales, disponibles en *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-092-17.pdf* y retomadas el 22 de julio de 2017, disponibles en *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-229-17.pdf.*

más altos de protección de información personal, actividades y funciones[98], y que dentro de nuestro país se encuentran en el ámbito de aplicación de la LFPDPPP.

Pareciera que, en caso de algún conflicto de tipo administrativo, es sencillo identificar el ámbito de competencia que correspondería a cada actor, así como las normas y procedimientos que resultarían aplicables a un caso concreto.

Sin embargo, no todas las situaciones de hecho se encuentran reguladas en las normas referidas dentro del marco jurídico nacional, de tal manera que la facultad de interpretación recae en los organismos responsables de velar por su cumplimiento, y en su caso, establecer parámetros o criterios que permitan orientar en el análisis de futuros casos.

Un ejemplo de lo anterior, y que probablemente ocurra en un mayor número de ocasiones, consiste en los problemas que podrían presentarse derivados de la implementación de la LGPDPPSO y las demás leyes estatales de la materia, ya que si bien las segundas deben observar las bases, principios y procedimientos establecidos en la primera, lo cierto es que los sujetos obligados de dichas normas, al pertenecer al sector público realizan tratamiento de datos personales de los habitantes de nuestro país, y en dicha acción existen figuras jurídicas como la transferencia, portabilidad, la creación de bases de datos, servicios de cómputo en la nube, o incluso convenios de colaboración que incluyan cualquier operación aplicada a datos personales.

En ese sentido, es cierto en la gran mayoría de ocasiones se establecen en las leyes, convenios o contratos, el ámbito jurisdiccional de aplicación en caso de

---

[98] Tal es el caso de buenas prácticas que llevan a cabo las empresas en el tratamiento de datos personales, o incluso la adopción de normas ISO, cuyo fin consiste en establecer especificaciones de productos, servicios y sistemas, para asegurar la calidad, seguridad y eficiencia en la industria de cualquier tipo a nivel mundial, emitidas por la Organización Internacional para la Estandarización (ISO por sus siglas en inglés), siendo un ente no gubernamental que emite esta clase de normas desde 1947, *https://www.iso.org/about-us.html* y *https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/isoinbrief_2015.pdf.*

conflicto entre los involucrados; no obstante, no debemos ser omisos en recalcar que el Titular de los datos personales siempre cuenta con el derecho de interceder en la defensa de la protección de su información personal.

De cualquier manera, las autoridades deben velar por la interpretación conforme[99], encaminado por el principio pro persona que se comentó líneas arriba, y en el caso de datos personales de niños, niñas y adolescentes procurar el interés superior del menor.

Otro tipo de conflicto competencial se presenta por la materia del asunto que se analiza o el sector que regula la autoridad. Un ejemplo que es palpable en México es el robo de identidad, ya que, ante este tipo de conductas, existen autoridades que en el ámbito de sus facultades cuentan con competencia para actuar al respecto.

Antes de mencionar qué autoridades podrían entrar en conflicto competencial respecto del fenómeno del robo de identidad, es necesario señalar que éste se presenta si "una persona obtiene, transfiere, posee o utiliza de manera no autorizada datos personales de alguien más, con la intención de asumir de manera apócrifa su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero en detrimento de sus finanzas"[100].

---

[99] Si bien este término es complejo de definir, puede considerarse que por interpretación conforme se puede entender como "la actividad que consiste en buscar explicaciones de varios textos, por lo menos de dos, que sean compatibles entre sí. En otras palabras, su objetivo consiste en identificar una o más interpretaciones conformes como resultado de dicha acción". Rodríguez, Gabriela et. al., *Interpretación conforme*. México, Comisión de Derechos Humanos del Distrito Federal - Suprema Corte de Justicia de la Nación - Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2013, p. 7, *http://www2.scjn.gob.mx/red/coordinacion/archivos_Interpretacion.pdf*

[100] Amigón, Edgar, "Robo de identidad, un delito en aumento", *Proteja su dinero,* México, CONDUSEF, núm. 186, septiembre 2015, p. 23, *http://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf*

En otras palabras, se trata de un delito que tiene lugar cuando alguien se hace pasar por otra persona, con el fin obtener o transferir datos personales de cualquier índole para llevar a cabo diversas conductas a nombre de la víctima, por medio de los cuales le es posible cometer otros actos ilícitos, como es el caso de fraudes.

Ahora bien, es necesario aclarar al lector que, hasta la fecha, dentro del marco jurídico mexicano, a nivel federal no existe un tipo penal denominado robo de identidad o suplantación de identidad en Internet, por lo que evidentemente tampoco existe respecto de la identidad de menores, siendo que como ya se mencionó es un problema actual y completamente serio.

No obstante, en algunas de las entidades federativas de México, se ha regulado esta conducta[101], por ejemplo, la Ciudad de México tiene dentro de su código penal, un capítulo denominado "Usurpación de Identidad"[102], cuyo único artículo especifica el tipo penal de la usurpación de identidad, y que se realice por cualquier medio, lo cual abre la oportunidad para que se intente perseguir este tipo de conductas frente a las autoridades correspondientes.

---

[101] Conforme a la Guía para prevenir el robo de identidad, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, son 19 entidades federativas las que cuentan con regulación de este tema. Disponible para su consulta en *http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf*

[102] Código Penal para el Distrito Federal "Artículo 211 Bis. - Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa.
Se aumentarán en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo." disponible en línea: *http://www.aldf.gob.mx/archivo-5b523887b84cba9b46e165101d758f01.pdf*.

A pesar de lo anterior, es claro que todas las personas cuentan con otros mecanismos para actuar frente al robo de identidad y que líneas más abajo se indicarán.

De esta manera, es claro que el Estado es el responsable de garantizar los derechos fundamentales de todas las personas y que tiene un rol vital por el cumplimiento de este deber, por lo que, en la misma línea de argumentación presentada en párrafos anteriores, considero que es necesario proteger los derechos de los menores, considerando en todo momento su interés superior.[103]

Así que, respecto de las autoridades competentes en esta materia, se encuentre en un primer momento el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, institución que dentro de sus principales objetivos está el de garantizar el derecho a la protección de datos personales. En ese sentido, si el titular de los datos ejerce sus derechos ARCO ante la entidad del sector público o privado que haya hecho un mal tratamiento de sus datos personales, y que haya derivado en el robo de identidad, y no queda conforme con la atención a su trámite puede acudir ante dicho Organismo Garante e iniciar, en el caso del sector privado un procedimiento de protección de derechos o un procedimiento de verificación conforme a la LFPDPPP o un recurso de revisión en el caso del sector público conforme a la LGPDPPSO.

Tal es el papel de este actor en esta clase de problemas que, el presente año este Organismo Autónomo emitió la Guía para prevenir el robo de identidad, documento con el que se busca “proporcionar información relevante con relación al

---

[103] De acuerdo con Miroslava Carrillo Martínez “es imperativo que el Estado se coloque a la vanguardia de los avances tecnológicos, para prevenir y sancionar las conductas que vulneran los derechos humanos y, específicamente, el derecho a la protección de los datos personales.” Carrillo, Miroslava, “Políticas públicas para proteger los datos personales de los menores en internet y en redes sociales”, *Retos de la protección de dato personales en el sector público,* México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011, p. 276*, http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf.*

robo de identidad, con la finalidad que las personas cuenten con herramientas para conocer cómo proteger sus datos personales y así poder reducir el riesgo de que su identidad sea robada"[104].

En segundo plano, se ubica la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) cuyo ámbito de aplicación queda fuera de lo previsto en la LFPDPPP, cuyo artículo 2, fracción I, exceptúa de ser sujetos regulados por la misma a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables.

Si la información que se sustrajo para cometer el robo de identidad es del sector financiero, es decir, aquella vinculada con cuentas bancarias, tarjetas de débito o crédito, o cualquier otra operación de dicha índole, y cuyos datos fueron tratados por alguna institución financiera, el afectado puede acudir ante dichas instancias para solventar su problema y su defecto, ante una respuesta insatisfactoria, puede presentar la queja correspondiente ante la CONDUSEF.

La tercera autoridad que también cuenta con competencia para actuar debido al robo de identidad es la Procuraduría Federal del Consumidor (PROFECO) en los casos que la información obtenida se haya utilizado para la contratación de bienes o servicios, de tal manera que, para inconformarse por esta clase de actos en el comercio, se puede iniciar un procedimiento de denuncia ante dicha institución.

Es tal la vinculación entre los tres entes gubernamentales que se han hecho diversas acciones enfocadas a disminuir la cantidad de casos de robo de identidad y mejorar el actuar de los servidores públicos[105].

---

[104] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para prevenir el robo de identidad*, México, 2017, p.4, *http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf*

[105] Tal es el caso de Convenios de colaboración, como el hecho en 2016 entre el INAI y la CONDUSEF, cuyo objeto consiste básicamente en establecer mecanismos de coordinación para que en el ámbito de sus respectivas competencias realicen acciones en materia de protección de datos personales ante posibles actos de

Por otro lado, tanto a nivel jurisdiccional e incluso internacional es posible localizar casos en los que existan conflictos competenciales, cuyos criterios de interpretación y niveles de protección podrían resultar desiguales en materia de protección de datos personales.

Sin embargo, en junio de 2017 la Red Iberoamericana de Protección de Datos emitió, en el marco del XV Encuentro de dicha Red, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, de los cuales forma parte México, representado por el INAI.

El objeto de los Estándares mencionados consiste, en los siguientes cinco puntos[106]:

1. Establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región
2. Elevar el nivel de protección de las personas físicas en lo que respecta al tratamiento de sus datos personales, el cual responda a las necesidades y

---

usurpación de identidad, disponible para su consulta en *http://inicio.ifai.org.mx/ConveniosInstDocs/CONV-40-2016%20Procuraduria%20Federal%20del%20Consumidor%20PROFECO.pdf.* Por otro lado, la CONDUSEF y la PROFECO también firmaron un convenio de colaboración para la homologación de criterios frente a entidades financieras y comerciales, además de establecer medidas preventivas coordinadas frente a diversas conductas como el robo de identidad. Lo anterior conforme al boletín de prensa 0058 de PROFECO, disponible para su consulta en: *https://www.profeco.gob.mx/prensa/prensa16/junio16/bol00058.php*

[106] Red Iberoamericana de Protección de Datos, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos,* junio 2017. Disponibles para su consulta en *http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf*

exigencias internacionales que demanda el derecho a la protección de datos personales.

3. Garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes.
4. Facilitar el flujo de los datos personales entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento social y económico de la región.
5. Impulsar el desarrollo de mecanismos para la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, autoridades de control no pertenecientes a la región y autoridades y entidades internacionales en la materia.

Naturalmente, diferencias como el tipo de legislación, sistema jurídico, niveles de seguridad, atribuciones de las autoridades responsables en cada uno de los Estados, fueron algunas causas por las que se emitieron estos Estándares, por lo que resulta muy interesante verificar en los siguientes años la adopción que han tenido los Estados Iberoamericanos y en su caso, si es posible contar con niveles de protección de datos personales como los impulsados en la Unión Europea.

No pasa desapercibido que el numeral 8 de los Estándares referidos establece respecto del tratamiento de datos personales concernientes a niñas, niños y adolescentes, que se debe privilegiar la protección del interés superior de éstos, conforme a la Convención sobre los Derechos del Niño y demás instrumentos internacionales que busquen su bienestar y protección integral, incluyendo la promoción educativa del uso responsable, adecuado y seguro de las TIC y los eventuales riesgos a los que se enfrentan en ambientes digitales respecto del tratamiento indebido de sus datos personales, así como el respeto de sus derechos y libertades.

2.5. Resoluciones no vinculatorias en materia de protección de datos en redes sociales (buenas prácticas)

Ahora bien, si bien ya se analizó el marco jurídico nacional e internacional en materia de protección de datos menores, no se debe omitir el pronunciamiento respecto de las buenas prácticas tanto en el sector público como en el privado.

Si bien en diferentes campos de investigación y de trabajo se utiliza el término "buenas prácticas", existe una ambigüedad entre lo que debemos entender por dicho concepto.

En este sentido el INAI las define como "aquellas técnicas o métodos para el debido tratamiento de datos personales que han probado alcanzar buenos resultados para la organización y los titulares de los datos personales, y que pueden ser utilizadas como referencias para otras organizaciones con características similares"[107].

Las buenas prácticas resultan una herramienta novedosa y en la mayoría de los casos sin estar previamente diseñadas o establecidas por algún ente regulador. Su utilidad permite que los responsables durante el tratamiento de datos personales eleven la calidad de sus servicios y de sus niveles de protección, sin actuar en contra de sus obligaciones legales.

Así, permiten que tanto los responsables, titulares de datos personales y autoridades garantes del derecho de protección de datos personales participen en un ambiente que, frente al tratamiento de los datos personales, se evite con certeza vulneraciones a este tipo de información, teniendo por consecuencia beneficios para el responsable por su imagen y reconocimiento que otorguen clientes y autoridades.

Con las buenas prácticas los diversos integrantes de la sociedad que traten datos personales y que a su vez forman parte de un mismo sector, se incentiva a mejorar el tratamiento de información personal, e incluso diseñar nuevos esquemas o acciones que aumenten el beneficio tanto para el responsable, como a los titulares de los datos personales.

---

[107] Tomado del glosario contenido en la Convocatoria del Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales 2017 del INAI, disponible para su consulta en *http://premioinnovacionpdp.inai.org.mx/Pages/Convocatoria-y-bases.aspx*

Precisamente, como el propio término lo indica, debe de realizarse, llevarse a cabo o ejecutarse, por lo que no puede ser únicamente un propósito o algo que no se haya presentado.

Los tipos de buenas prácticas, así como el alcance que puedan tener varían de acuerdo a los tipos de datos que recaba el responsable y al fin que éste les otorgue; pueden diseñarse desde sistemas automatizados que organicen los datos personales en un formato estructurado, programas que permitan el ejercicio de los derechos ARCO de manera expedita o cualquier otra herramienta que mejoren la eficacia del responsable al momento de cumplir con las obligaciones que establece la normatividad en la materia.

Es importante conocer las buenas prácticas que existen en nuestro país y mucho más en otros, ya que, si bien la normativa aplicable puede ser diferente en cada Estado, lo cierto es que en todos ellos se lleva a cabo tratamiento de datos personales, por lo que éste puede replicarse en las diferentes sociedades del planeta, incluyendo toda clase de mejoras y evitando los errores o fallas.

Además, debemos recordar que el derecho a la protección de datos personales es un derecho fundamental, y por tal motivo, cada persona tiene derecho a su ejercicio tanto en el sector público como en el privado, y si la legislación aplicable no permite o no regula determinada situación relacionada con el tratamiento de datos personales, considero que una buena manera de proteger nuestra información o llevar a cabo el uso, recolección, análisis, entre otras conductas respecto de los datos personales como responsables de los mismos, se presenta con la implementación de prácticas que han sido favorables en otros lugares del mundo.

Al respecto, es claro que para determinar que una conducta es una buena práctica, tuvo que iniciar con ensayo-error durante el tratamiento de datos personales a cargo de un responsable, de tal manera que, cada una puede ser perfectible teniendo por consecuencia que los responsables garanticen de mejor manera el derecho a la protección de datos personales.

A continuación, se mencionarán algunas buenas prácticas en materia de protección de datos personales tanto en México como en otros países:

a) México

CREDENCIAL [NO SOLO] PARA VOTAR IMPLEMENTACIÓN DE BUENAS PRÁCTICAS EN MATERIA DE DATOS PERSONALES EN EL REGISTRO FEDERAL DE ELECTORES[108].

Esta práctica en nuestro país maneja conceptos fundamentales como el tratamiento de datos personales fotografía, firma, domicilio, CURP, datos biométricos, entre otros, generando un derecho a la identidad, por medio de la Credencial para Votar con Fotografía, así como ofrecer un listado de los servicios inherentes al control, actualización y verificación de la emisión de dicho documento.

Así, el Instituto Nacional Electoral (INE), a través de la Dirección Ejecutiva del Registro Federal de Electores, implementó el Servicio de Verificación de Datos de la Credencial para Votar, para que las instituciones públicas y privadas estén en posibilidad de cotejar la información concerniente al ciudadano en términos de su vigencia y autenticidad.

Con este servicio se puede: a) Verificar la vigencia y cotejar los datos de la credencial para votar que presenten los ciudadanos para identificarse ante una institución pública o privada, respecto de la información almacenada en los registros del Instituto. b) Autenticar las huellas dactilares del ciudadano que se identifique con una Credencial para Votar, mediante la comparación de las marcas dactilares capturadas al momento de presentar la credencial con aquellas que se encuentran almacenadas en los registros del Instituto.

Algunas de sus características consisten en lo siguiente:

1. Establece mecanismos y esquemas de seguridad, como son: cifrado de información a través de llaves públicas y privadas, enlace dedicado entre la Institución pública o privada y el INE, a través de los cuales se realiza, en tiempo real, la recepción de los datos contenidos en la CPV y respuesta de validación de los mismos.

---

[108] Disponible en: *http://premioinnovacionpdp2016.inai.org.mx/Ganadores/Folio%2032%20INE.pdf*

2. Para la autenticación de la huella dactilar, realiza la confrontación de la información proporcionada por la institución pública o privada, con la que se tiene en los registros del Instituto mediante un método de comparación de la información de huellas dactilares, que da como respuesta un porcentaje de similitud.
3. No expone datos del Padrón Electoral como parte del proceso de verificación, ya que, en ningún caso y bajo ningún motivo proporciona información de los ciudadanos y en ningún momento se tiene acceso a la información de la base de datos que está en posesión del Instituto, ni a sistemas internos de información.
4. Promueve la interacción con instituciones públicas o privadas otorgándoles certeza sobre la identidad del ciudadano al momento de solicitar la prestación de bienes y/o servicios, garantizando en todo momento la efectiva protección y confidencialidad de los Datos Personales de los ciudadanos.

En este sentido, si bien se han propuesto diversos instrumentos de identificación de los menores, lo cierto es que hasta la fecha ninguno ha tenido éxito, por lo que no ha sido posible identificar mejores prácticas al respecto en nuestro país.

Un ejemplo de lo anterior, es el documento de identificación derivada del Registro de Menores de Edad, contemplado en el artículo 89 en relación con el 111 de la Ley General de Población[109], y que su Reglamento denominó Cédula de Identidad Personal, misma que contendría los siguientes datos personales: a) Nombre completo; b) Sexo del o la menor; c) Lugar y fecha de nacimiento; d) Nombres completos del padre y la madre; e) Clave Única de Registro de Población;

[109] Artículo 89.- El Registro de Menores de Edad, se conforma con los datos de los mexicanos menores de 18 años, que se recaben a través de los registros civiles. Artículo 111.- La Secretaría de Gobernación podrá expedir un documento de identificación a los mexicanos menores de 18 años, en los términos establecidos por el reglamento de esta ley. Disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/pdf/140_011215.pdf*

f) Fotografía del titular; g) La codificación de la imagen del iris, y h) Lugar y fecha de expedición.[110]

USO DEL PROGRAMA PLAZA SÉSAMO: MONSTRUOS EN RED.

Mediante acuerdo número ACT-PUB/25/10/2016.06[111], aprobado por el Pleno del INAI el 25 de octubre de 2016, este Organismo Garante autorizó la celebración de un contrato plurianual para la adquisición de la licencia para el uso del programa Plaza Sésamo: Monstruos en Red.

Dicho programa consiste en una iniciativa en múltiples plataformas (serie de televisión, guías interactivas, juegos en línea, libros electrónicos, entre otros), diseñada para apoyar a niños y niñas, familias y educadores en la formación de buenos hábitos de uso y aprovechamiento de las nuevas tecnologías de la información y las comunicaciones[112].

Como resultado de dicho contrato, se ha implementado un programa que se transmite en televisión y en Internet[113], cuyo objetivo es difundir contenidos relacionados con la protección de datos personales de menores y la navegación segura en Internet.

Con esta clase de buenas prácticas, el Organismo Garante del derecho de protección de datos personales, lo promueve y procura generar concientización respecto del uso de datos personales de menores en Internet, incluyendo las redes

---

[110] Lo anterior conforme al artículo 54 del Reglamento de la Ley General de Población, disponible para su consulta en *http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LGP.pdf.*

[111] Disponible para su consulta en *http://inicio.ifai.org.mx/AcuerdosDelPleno/ACT-PUB-25-10-2016.06.pdf*

[112] Esto conforme al Anexo Uno del Acuerdo ACT-PUB/25/10/2016.06 del INAI.

[113] Es transmitido a través del Canal Once del Instituto Politécnico Nacional y en Internet, a través del siguiente vínculo electrónico *https://www.youtube.com/watch?v=7xyCGCwKePM&list=PL1vMhg3AawgTfbsZ6zsOiDjwZ5VleQ4u9*

sociales, teniendo por consecuencia el desarrollo de la cultura de la protección de datos personales, así como el uso responsable de las TIC.

b) España

CÓDIGO DE BUENAS PRÁCTICAS EN PROTECCIÓN DE DATOS PARA PROYECTOS BIG DATA[114]

Derivado del uso de Big Data, entendido como el "conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo"[115], es claro que se tratan datos personales de millones de personas, de tal manera que, con base en el imperativo tecnológico, resulta imperante la generación de buenas prácticas.

Cada uno de los procesos que involucre Big Data utilizará grandes fuentes de datos, en las que se procurará primordialmente la nula identificación de los titulares de los datos personales que se utilizaron. En estos casos nos encontraremos ante buenas prácticas que, a pesar del uso de Big Data, se evita la vulneración a la privacidad de las personas.

Conforme al mencionado código se considerarán buenas prácticas las siguientes[116]:

- La metodología de Protección de Datos desde el Diseño, es decir de manera previa a la implementación de algún sistema o instrumento que trate datos personales debe de llevarse a cabo un análisis del impacto que conlleva su

---

[114] Disponible para su consulta en *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf*

[115] Agencia Española de Protección de Datos y Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, *Código de buenas prácticas en protección de datos para proyectos big data*, España, 2017. P. 3, *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf*

[116] Ibídem, Pp. 30-31

tratamiento previo a su realización, con el fin de evitar vulnerar la autodeterminación informativo del dueño de los datos que se tratarían en un futuro.

- Hay que valorar el uso de la anonimización en relación a los requisitos previos o contexto y los objetivos o finalidad de ese proceso, revisando periódicamente e igualmente evaluando los posibles nuevos riesgos que puedan surgir como consecuencia de diferentes factores, como el desarrollo de nueva tecnología.
- Las técnicas de anonimización deben preservar la utilidad de los datos en la medida de lo posible, por el que puedan replicarse para casos futuros como los que se presentan en la elaboración de perfiles.
- No confundir entre seudonimización y anonimización, ya que la primera es una técnica en la que se reemplaza un atributo por otro en un registro, disminuye el riesgo de identificación del titular del dato, pero se mantiene la posibilidad de identificarlo con otros elementos, por tanto, es una medida de seguridad útil a usar como paso intermedio en un proceso de anonimización.
- Establecer medidas de seguridad dentro del proceso de anonimización, como es el caso de auditorías periódicas de las fuentes de información, además de incluir procedimientos de posibles brechas de privacidad que pudieran surgir, como casos de re-identificación.
- Adoptar códigos de conducta que conlleve el cumplimiento de la legislación vigente, certificaciones, u otros estándares que permitan identificar al responsable como un ente cuya privacidad de sus clientes sea primordial, lo cual le permitiría obtener un mayor lugar en el mercado.

En este caso, es evidente el uso de Big Data en Internet, cuya fuente de información puede localizarse en redes sociales; por este motivo, si los responsables de los datos personales garantizan el cumplimiento a la normativa vigente y además impulsan el uso de buenas prácticas como las indicadas, ellos junto con los titulares de los datos se verían beneficiados por la protección que se presente a sus datos personales, y más tratándose de menores de edad, en cuyo

caso, con el paso del tiempo se presentan mayores cantidades de información que las empresas utilizan a través de Big Data.

A pesar de la identificación de algunas buenas prácticas, se visualizan importantes desafíos en materia de difusión de los principios y obligaciones que se derivan de la normativa vigente en materia de protección de datos en el área de la investigación.

c) México (sector privado)

SISTEMA DE CONTROL DE VISITANTES.[117]

El sistema de control de visitantes, SCV, para condominios u oficinas públicas y privadas busca abatir con el problema derivado del acceso a conjuntos residenciales, oficinas públicas y privadas en las que el registro de visitantes no cumple con los principios y obligaciones de la normativa aplicable al sector público y privado.

SCV tiene como objetivos principales: 1) Proteger los datos personales tanto de los invitadores como de los visitantes. 2) Agilizar el registro y acceso de visitantes evitando las largas filas que en ocasiones se forman en los puntos de acceso 3) Aumentar la seguridad de los residentes en relación a los visitantes que pueden ingresar al conjunto habitacional u oficina al tener un control preciso de quiénes pueden dar accesos al establecimiento y el momento de entrada y salida de los visitantes.

Características:

- Funciona mediante un software y una app de manera fácil y rápida.
- Inicia con la captura de la estructura del condominio u oficina (unidades habitacionales o áreas de oficina, residentes o empleados y su asignación específica).
- El segundo paso es enviar un correo personalizado para que se registren las personas autorizadas a dar acceso al establecimiento en el sistema.

[117] Disponible para su consulta en *http://premioinnovacionpdp2016.inai.org.mx/Ganadores/Folio%2022%20SLVCI.pdf*

- El residente o empleado autorizado, ahora como invitador, ingresa los datos de sus visitantes y emite pases de visita que contiene información sobre el invitado, el invitador y un código QR. Estos pases los puede emitir desde la página o desde una aplicación en su teléfono inteligente.
- Los guardias o personal asignado a los escritorios de registro escanean el código con una aplicación, misma que le informa si es un pase válido y dependiendo de las políticas del centro, puede tomar la fotografía del visitante, así como de su identificación, placa vehicular y datos de equipo de cómputo.
- Cuando el visitante registra exitosamente su entrada, el invitador recibe una notificación en su teléfono inteligente y un correo anunciándole la llegada de su invitado.
- Cuando el visitante registra su salida, se le envía un correo electrónico al invitador.
- En cada una de las fases del uso de la plataforma: registro, envío de pase, lectura de pase, los datos de los involucrados están protegidos para que sean vistos sólo por los roles apropiados.
- De igual forma, los invitadores e invitados pueden consultar el aviso de privacidad y ejercer sus derechos ARCO.

En este sentido, es dable presumir que en cualquier edificio que involucre el registro de visitantes, incluirán datos personales y, tratándose de información de menores de edad, es mayor el nivel de protección que deben de tener los responsables de dichos sistemas, toda vez que en la mayoría se involucran datos biométricos, y que, conforme a la normativa vigente en la materia, se consideran datos personales sensibles.

2.6. Resolución del grupo de trabajo Artículo 29 en materia de protección de datos en redes sociales (Dictamen 5/2009 sobre las redes sociales en línea).[118]

Este documento se adoptó el 12 de junio de 2009, conforme a lo establecido por la Directiva 95/46/CE del parlamento europeo y del consejo de 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[119], y entre otras cosas analiza cómo la evolución de los servicios en internet cambia el tratamiento de datos personales, de tal manera que el número de usuarios de las redes sociales se ha incrementado de manera exponencial.

Así las cosas, cualquier información que se publica junto con sus descripciones y demás datos relacionados con ésta, permiten crear perfiles de los usuarios, a partir de las herramientas que crean las redes sociales, por lo que las recomendaciones emitidas en el dictamen son aplicables a todos los proveedores de servicio de redes sociales, aunque se encuentre su sede fuera del Espacio Económico Europeo (EEE)

Expresa que los proveedores de redes sociales son los responsables del tratamiento de datos personales ya que sus actividades en las que utilizan esta

---

[118] Si bien es cierto que se emitió el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y que este documento se elaboró con base en la derogada Directiva 95/46/CE, para efectos de este documento resulta muy útil el análisis que se realiza del tratamiento de datos personales en redes sociales, el cual resulta aplicable actualmente a pesar del cambio normativo indicado. El documento se encuentra disponible para su consulta en *http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf*

[119] Disponible para su consulta en *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf*

información, implica desde el registro hasta la supresión de la cuenta, disponer de ellos para fines publicitarios e incluso cuando se vincula el perfil con otras aplicaciones que tratan datos personales.

No obstante, dentro de las redes sociales, existen usuarios que manejan datos personales de terceros para fines distintos al uso particular o doméstico, de tal manera que además de ser usuario, comparten la calidad de responsable respecto de los datos que hayan recabado para otros fines de tipo comercial, político o social.

Pese a la mencionada exención doméstica, establece la posibilidad consistente en que un usuario se vuelva responsable de conformidad con lo establecido en el derecho civil o penal nacional, por situaciones que impliquen el tratamiento de datos personales como la difamación, responsabilidad por violación del derecho a la personalidad, o alguna responsabilidad penal.

Además, este dictamen retoma los principios de seguridad y de confidencialidad[120] que corresponden al actuar del responsable, cuyo cumplimiento puede exigirse por parte de los titulares.

[120] Estos deberes se han mencionado en múltiples instrumentos normativos y en algunos casos, como sucede en México, se han establecido como deberes en materia de protección de datos personales. Para efectos del presente documento se retoman las definiciones establecidas en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos del 20 de junio de 2017, conforme a sus artículos 21 y 23. Artículo 21. Principio de seguridad 21.1. El responsable establecerá y mantendrá, con independencia del tipo de tratamiento que efectúe, medidas de carácter administrativo, físico y técnico suficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos personales. Artículo 23. Principio de confidencialidad 23.1. El responsable establecerá controles o mecanismos para que quienes intervengan en cualquier fase del tratamiento de los datos personales mantengan y respeten la confidencialidad de los mismos, obligación que subsistirá aun después de finalizar sus relaciones con el titular

Respecto del primero, indica que deben de adoptarse las medidas técnicas y de organización apropiadas antes y durante la aplicación del servicio, que garanticen la seguridad e impedir el tratamiento no autorizado, previendo los riesgos que pudieran presentarse en el mismo, y por la naturaleza de los datos que se deben proteger.

En cuanto al segundo, establece que los responsables de los servicios de redes sociales, deben diseñar parámetros de confidencialidad en cuanto al acceso de los datos que cualquier persona ingresa en la plataforma, de tal manera que, por un lado, existan restricciones para los terceros que deseen acceder a la información del usuario sin su consentimiento, en su calidad de usuarios de la misma red social o a través de motores de búsqueda.

Por otro lado, indica que cada red social debe establecer parámetros por defecto respetuosos de la intimidad, y por consecuencia, los usuarios decidan libremente si cualquier persona distinta a sus contactos, pueda acceder a su perfil, permitiendo reducir el riesgo de un tratamiento ilícito por terceros, incluso sin que sea posible realizar una búsqueda por parámetros como la edad o el lugar.

En relación con la identidad del responsable, el grupo de trabajo recomendó que los proveedores de esta clase de servicios deberían informar a cada usuario su identidad, incluyendo los fines para los que tratan los datos personales, los posibles riesgos que impliquen un ataque a su intimidad por subir información en línea de ellos o de terceros que afecten su protección de datos, invitando a sus usuarios a la no publicación de fotografías o cualquier información de otras personas sin su consentimiento.

Como se comentó líneas arriba, Internet es una gran herramienta para el intercambio de información de cualquier tipo de manera inmediata, consultable desde cualquier dispositivo electrónico. En ese sentido, la protección de datos personales sensibles debe ser mayor en las redes sociales, ya que de acuerdo con este dictamen esta clase de información sólo puede publicarse con el consentimiento explícito de la persona interesada o sólo si el titular la ha hecho del conocimiento público.

Además, si el responsable de la red social desea recabar datos personales sensibles debe hacerlo previo a la obtención del consentimiento explícito y en su caso, hacer del conocimiento del titular que esta clase de transmisión de datos es voluntaria y no obligatoria para acceder al servicio.

Hay ocasiones en la que terceros tienen acceso a datos personales proporcionados por los usuarios de una red social ya que ocupan aplicaciones externas a la plataforma, pero que incrementan la calidad del servicio, de tal manera que los encargados de las redes sociales, deben garantizar que cualquier aplicación que se vincule con la suya cumpla con la normativa aplicable a la protección de datos y la privacidad, incluyendo las comunicaciones electrónicas.

Aunado a lo anterior, los responsables de cada red social deben ofrecer el acceso más limitado por parte de terceros e incluso, la posibilidad de expresar inquietudes de los usuarios respecto de cada aplicación. En este punto, conviene recordar que el principio de proporcionalidad[121] en materia de datos personales implica el recabar la información estrictamente necesaria para poder realizar el tratamiento correspondiente, evitando así el manejo de información personal distinta a la originalmente recabada para fines distintos, incluyendo la publicidad.

Para los casos en los que el usuario decide suspender el uso de la red social, el dictamen expresa que los servicios de estas plataformas conservan la información del perfil de la persona para evitar el nuevo registro de la misma, la cual sólo puede conservarse por no más de un año, sin almacenar las razones por las que se decidió suspender su cuenta electrónica.

En cambio, en las situaciones que impliquen la supresión de las cuentas (incluso por la inactividad por parte del usuario) deberían eliminarse todos los datos del usuario, de tal manera que no se conserven por parte del proveedor de la red

[121] Conforme al artículo 18 de los Estándares de Protección de Datos Personales para los Estados Iberoamericanos el Principio de proporcionalidad indica que el responsable tratará únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento.

social, salvo en casos que involucre razones jurídicas o de seguridad, o en su caso que impidan conductas como la usurpación de identidad o algún otro delito.

Ahora bien, en cuanto al ejercicio de los derechos ARCO, se indica el deber de permitirlo por parte de todas las personas físicas cuyos datos se tratan en la red social, sin importar si son usuarios o no.

Por último, en cuanto a los menores de edad, advierte que los servicios de redes sociales son utilizados por este sector de la sociedad, de tal manera que tal y como se estableció en la Convención internacional sobre los derechos del niño, debe prevalecer el respeto por el principio del interés superior del menor, sobre todo por lo que se refiere a los posibles riesgos que conlleva el uso de datos personales en redes sociales, a partir de soluciones como la comprobación de la edad requerida y la prueba del consentimiento informado para ser usuario.

El grupo de trabajo estableció una estrategia que permitiría abordar la protección de datos de los niños en las redes sociales, basada en los siguientes puntos:

- Iniciativas de sensibilización, fundamentales para garantizar el compromiso activo de los niños (mediante las escuelas, la inclusión en el programa escolar de elementos de protección de datos, la creación de herramientas educativas ad hoc y la colaboración de organismos nacionales competentes);
- Un tratamiento justo y legal frente a los menores, por ejemplo, no pedir datos sensibles en el formulario de registro, no realizar comercialización directa destinada específicamente a los menores, el acuerdo previo de los padres o tutores antes del registro, así como grados adecuados de separación lógica entre las comunidades de niños y de adultos;
- Instauración de tecnologías que mejoren la protección de la intimidad, es decir, parámetros por defecto respetuosos de la intimidad, ventanas emergentes de advertencia en fases adecuadas, así como programas informáticos de verificación de la edad;
- La autorregulación de los proveedores con el fin de fomentar la adopción de códigos de buenas prácticas que deberían incluir medidas de ejecución eficaces y sanciones disciplinarias;

- Sólo en caso necesario, medidas legislativas ad hoc para desalentar prácticas desleales y/o fraudulentas en el contexto de los servicios de las redes sociales.

2.7. Memorándum de Montevideo

Este instrumento derivó de los trabajos realizados dentro del Seminario Derechos, Adolescentes y Redes Sociales en Internet realizado en Montevideo, y se adoptaron diversas recomendaciones en la materia el 28 de julio de 2009[122], bajo dos premisas: 1) el reconocimiento que niñas, niños y adolescentes son titulares de todos los derechos, y podrán ejercerlos en función de su edad y madurez; 2) por su particular condición de desarrollo tienen el derecho a una protección especial en aquellas situaciones que pueden resultar perjudiciales para su desarrollo y derechos.

Las niñas, niños y adolescentes son sujetos especialmente protegidos y vulnerables respecto del tratamiento de sus datos personales, de los cuales los organismos multilaterales deben garantizar sus derechos y enfocar esfuerzos para promover o fortalecer una cultura de protección de datos en las niñas, niños y adolescentes.

Así, teniendo en claro que el Internet y las redes sociales son herramientas útiles para el ejercicio de los derechos de los menores, se adoptan estas recomendaciones a partir del conocimiento de los riesgos y peligros a los que este sector de la sociedad se encuentra expuesto.

Esto a partir del reconocimiento del papel que cumple la familia, o quien cuide a los menores sobre el uso responsable y seguro de herramientas como Internet,

[122] Utilizan como referente normativo fundamental la Convención sobre los Derechos del Niño, misma que fue ratificada por todos los países de la región, adquiriendo así la responsabilidad compartida de la sociedad y el Estado en la protección de la infancia y la adolescencia. Por lo que este instrumento internacional es aplicable para dichos países. Disponible para su consulta en: http://clicseguro.sep.gob.mx/archivos/Memorandum_Montevideo.pdf

incluyendo redes sociales digitales; la necesidad de que todas las medidas que se tomen prioricen el interés superior de niñas, niños y adolescentes, que todo aquel que se beneficie de cualquier forma de Internet y de las redes sociales digitales son responsables por los servicios que proveen, por tanto deben asumir su responsabilidad en las soluciones a la problemática que se presente.

En el memorándum indicado, se especifica que se debe transmitir claramente a las niñas, niños y adolescentes que Internet no es un espacio sin normas, impune o sin responsabilidad, por lo que la participación anónima o el uso de pseudónimos, debe involucrar el respeto a la privacidad, intimidad y buen nombre de terceras personas, responsabilidades civiles, penales y administrativas que existen cuando se vulneran derechos propios o de terceros en la red, entre otros aspectos.

Las recomendaciones se encuentran dirigidas a diversos actores que participan en el desarrollo de los menores de edad y su convergencia con herramientas digitales como Internet y redes sociales, es decir el Estado a través de instituciones educativas y las autoridades que aplican la ley (incluidas las de protección de datos personales), la industria y cualquier otro sector de la sociedad que tenga participación en Internet y el tratamiento de datos personales.

Además, incluyen recomendaciones enfocadas a la prevención de los riesgos que corren los menores de edad, así como a la emisión de políticas públicas que protejan datos personales de este sector social dentro de las redes sociales.

Por lo anterior, el resultado de las recomendaciones que se adoptaron en Montevideo en julio de 2009, muestran el vínculo que existe entre sociedad civil, la industria y el Estado en el desarrollo integral de los menores, ya sea garantizando el ejercicio de sus derechos a través de herramientas de comunicación como Internet y redes sociales digitales, o protegiéndolos de los riesgos y peligros a los que se encuentran expuestos en la red de redes.

Capítulo 3

Políticas de privacidad y recomendaciones

Capítulo 3: Políticas de privacidad y recomendaciones

3.1 Análisis de políticas de privacidad en redes sociales, de acuerdo a la zona geográfica

En este apartado se analizarán diversas políticas de privacidad de redes sociales en Internet, en especial respecto del mínimo de edad para ser usuario de cada una, y en su caso si existe una sección aplicable directamente a los niños, niñas y adolescentes.

Facebook.

Esta red social cuenta con mayor presencia en el mundo, ya que de los 7,600 millones de personas que habitan el planeta[123], esta plataforma cuenta con más de 2000 millones de usuarios, motivo por el cual es viable presumir que es la plataforma que más trata datos personales sin importar su ubicación, sin mencionar los demás servicios o aplicaciones que utilizan su infraestructura para ofrecer otros productos.

De esta manera, Facebook cuenta con diversas políticas especializadas a determinados sectores de su funcionamiento, tales como datos personales (privacy)[124], cookies[125], seguridad[126], y las condiciones del servicio[127]. Las últimas mencionadas, establecen derechos y responsabilidades de los usuarios de Facebook sin importar su ubicación, las cuales versan sobre las implicaciones que derivan del uso de la misma, desde su registro, la información que recaban y tratan, la publicidad que ofrece, la terminación del servicio, entre otros aspectos.

Así las cosas, el apartado 4 denominado “Registro y seguridad de las cuentas” establece ciertos deberes por parte de los usuarios de Facebook en cuanto

---

[123] Cantidad informada la Organización de las Naciones Unidas en junio de 2017, disponible para su consulta en *https://www.un.org/development/desa/es/news/population/world-population-prospects-2017.html*

[124] Disponible para su consulta en *https://www.facebook.com/about/privacy/*

[125] Disponible para su consulta en *https://www.facebook.com/policies/cookies/*

[126] Disponible para su consulta en *https://www.facebook.com/help/safety*

[127] Disponibles para su consulta en *https://www.facebook.com/legal/terms/update*

a la información que proporcionan sus usuarios, tales como no crear una cuenta para otras personas sin su autorización (incluyendo a padres respecto de sus hijos), la prohibición de usar esta red social si se es menor de 13 años, o si fue declarado culpable de un delito sexual, entre otras cosas.

Cabe señalar que, dentro de los apartados de Facebook, estableció un módulo dentro de su centro de seguridad, enfocado a la prevención del bullying[128] en el que pueden intervenir adolescentes (de acuerdo con la prohibición señalada en el párrafo anterior), padres de familia y educadores, cada uno desde el ámbito que le corresponda, brindando ayuda mediante consejos y acompañamiento para prevenir o erradicar esta clase de conductas.

También cuenta con otro portal encaminado al conocimiento de Facebook por parte de los padres o tutores, en el que se encuentran de manera simple las herramientas que lo conforman y consejos de expertos en seguridad en Internet[129].

Así las cosas, Facebook ha tratado de inhibir el uso de su red social por personas menores a 13 años, así como la eliminación de conductas violentas como el bullying; no obstante, en la actualidad es factible localizar cuentas de usuarios que son administradas por menores de edad, o por alguno de sus familiares y peor aún, podemos localizar contenido enfocado a la violencia en contra de cualquier persona y especialmente de menores de edad.

Por lo anterior, los demás usuarios tenemos otra clase de recursos que la misma red social desarrolla para evitar cualquier actividad o conducta que afecte el desarrollo de los menores de edad en Internet, tal es el caso de buenas prácticas dentro de Facebook y en casos más estrictos, como el reporte de cualquier contenido que se genere, de tal manera que se revisa el contenido reportado y elimina todo lo que infrinja las normas comunitarias o demás condiciones que establece en sus servicios y productos.[130]

---

[128] Disponible para su consulta en *https://www.facebook.com/safety/bullying*

[129] Disponible para su consulta en *https://www.facebook.com/safety/parents*

[130] La configuración correspondiente a cómo reportar contenido se encuentra disponible en: https://www.facebook.com/help/181495968648557/?ref=sc

Messenger kids

Esta nueva aplicación[131] fue diseñada por Facebook con características que permiten reconocer el deber de los desarrolladores de las TIC en el ejercicio de los derechos de los niños dentro de Internet y que tiende a ser más segura la interacción entre otros usuarios con edades similares a la suya. Se trata de una aplicación sin publicidad, controlada por los padres de los menores desde su cuenta de Facebook, que permite a los usuarios enviar mensajes o imágenes, así como realizar video llamadas con los contactos aprobados por los padres o tutores.

Cabe señalar que, hasta la fecha, únicamente se encuentra disponible en Estados Unidos para dispositivos Apple (Ipad, Ipod Touch o Iphone) y posteriormente se permitirá su descarga para equipos Android o de la compañía Amazon. Asimismo, esta aplicación es compatible con la norma relativa a la protección de los niños en Internet de Estados Unidos, es decir la *Children's Online Privacy Protection Act* (COPPA).

De acuerdo con sus términos de uso[132], la aplicación es exclusiva para niños que deseen comunicarse con familiares y amigos (previamente aprobados por los padres o tutores) en un ambiente seguro

También establece que los padres o tutores aceptan que Facebook pueda recolectar, usa y compartir los contenidos e información que se genere dentro de la aplicación de acuerdo con su política de privacidad, aclarando que en ambos casos le pertenece al menor de edad, no obstante, los padres o tutores otorgan permisos “en nombre de sus hijos) para, entre otras cosas, su uso a nivel mundial de manera gratuita sin la obligación de compensarlos de cualquier manera.

Al igual que en Facebook, Massenger kids se ajusta a las normas comunitarias, por lo que el menor de edad no debe publicar información que las

[131] Disponible para su consulta y descarga en https://messengerkids.com/

[132] Los términos de uso de Messenger Kids se encuentran disponibles en la página de Facebook en el siguiente vínculo electrónico: *https://www.facebook.com/help/1954771561401423*

contravenga incluidas los contenidos que promuevan el bullying, discrimine o cualquier otra que dañe a los demás usuarios.

Resulta importante señalar que, si bien la aplicación resulta diseñada para niños, los términos de uso de la misma, establecen que los menores de 13 años no deben registrarse sin el consentimiento de sus padres o tutores; sin embargo, no existe una edad mínima para ser usuario de Messenger Kids.

Por otro lado, respecto de las políticas de privacidad[133] es evidente que resultan muy similares a las de Facebook; sin embargo, al tratar datos de menores de edad establecen otros controles para la seguridad de los usuarios en la red de redes.

Los datos que recaba Messenger Kids abarcan la información que se encuentra en el perfil del usuario como el nombre, sexo, fecha de nacimiento, las comunicaciones y actividades que se llevan a cabo dentro de la aplicación, los contactos que tiene, así como la información del dispositivo en el que se encuentre instalada, que incluye el sistema operativo y la dirección IP, entre otros datos.

Facebook utiliza esa clase de información, conforme a su política de datos, para proveer, mejorar y desarrollar los servicios que ofrece, así como para promover la comunicación con los padres de familia o tutores, y determinar los contenidos que sean contrarios a lo establecido en sus términos de uso o en las normas comunitarias.

Es claro que, ante la novedad de esta aplicación, los demás desarrolladores de redes sociales busquen mejorar la experiencia de sus usuarios o en su caso, ofrecer diferentes servicios que les permitan competir con Facebook en la búsqueda de ampliar su cantidad de usuarios e innovar el mercado.

Twitter.

La famosa red social consistente en la publicación de mensajes de 140 caracteres o menos en tiempo real, estableció el “acuerdo de usuario de Twitter” el

---

[133] Disponibles para su consulta en *https://www.facebook.com/help/118909212153483*

cual está conformado por las Reglas de Twitter[134], su Política de privacidad y los Términos de servicio, en el que se enfocan en 3 líneas de desarrollo: 1) la posibilidad de publicar y compartir mensajes de manera instantánea; 2) el control de la información de la cual se consiente la recopilación y uso, incluida su transferencia a terceros; y 3) el respeto por los derechos de propiedad intelectual y la eliminación de cualquier contenido que promueva el odio o la explotación sexual infantil.

No obstante, Twitter cuenta con diferentes términos de uso si se reside fuera de los Estados Unidos. En el caso de los habitantes de dicho país que usen Twitter, deben tener al menos 13 años de edad[135]. En cambio, los términos de servicio de Twitter vigentes para los residentes en el resto del mundo, son omisos en establecer el mínimo de edad requerida para poder utilizar los servicios de esta red social[136].

En cuanto a la Política de Privacidad, establece que, sin importar el país de residencia del usuario, Twitter puede transferir, almacenar y usar la información recopilada en los Estados Unidos de América, Irlanda, y en cualquier otro país en el que opere.

Dentro de la información que recopila Twitter se encuentra el nombre, nombre de usuario, contraseña, dirección de correo electrónico o número de teléfono, así como cualquier otra información que derive de los contenidos que se publiquen o

---

[134] Disponibles para su consulta en *https://help.twitter.com/es/rules-and-policies/twitter-rules*

[135] Los términos de uso de Twitter para residentes de los Estados Unidos establecen lo siguiente: “You may use the Services only if you agree to form a binding contract with Twitter and are not a person barred from receiving services under the laws of the applicable jurisdiction. In any case, you must be **at least 13 years old to use the Services.”** “Puede utilizar los servicios sólo si acepta formar un contrato vinculante con Twitter y no está impedido de recibir servicios bajo las leyes de la jurisdicción aplicable. En cualquier caso, debe tener al menos 13 años para usar los servicios” (traducción propia), disponible para su consulta en *https://twitter.com/tos?lang=en*

[136] Disponible para su consulta en *https://twitter.com/es/tos#updateintlWho*.

de las personas con las que se interactúe como contactos, ubicación, sitio web, fecha de nacimiento, fotografía, entre otros.

Como se mencionó líneas arriba, Twitter establece restricciones a determinados contenidos dentro de su plataforma, tales como violencia gráfica, es decir aquella que muestre cualquier tipo de contenido multimedia que muestre muertes, lesiones graves, violencia o procedimientos quirúrgicos sangrientos, o cualquier otro contenido no apto para menores de edad, es decir aquel contenido multimedia que sea pornográfico o cuyo fin sea generar excitación sexual[137].

Para esta clase de contenidos es factible solicitar que se eliminen los contenidos que incluyan violencia gráfica excesiva por respeto a los fallecidos y a sus familiares, en el caso de que recibamos una solicitud de los familiares o de un representante autorizado.

Instagram

Esta red social consistente en la publicación de imágenes o videos con el uso optativo de filtros de edición, establece en sus condiciones de uso[138] que para ser usuario de los servicios se debe ser mayor de 14 años de edad, y no es posible publicar fotos u otro tipo de contenido que muestre imágenes violentas, de desnudos íntegros o parciales, discriminatorias, ilegales, transgresoras, de mal gusto, pornográficas o con contenido sexual.

A su vez, Instagram prohíbe la creación de una cuenta para nadie que no sea el usuario mismo, provocando que toda la información que se suministre durante el registro y en cualquier otro momento será verdadera, precisa, actual y completa, garantizando su actualización según sea necesario para mantener su veracidad y precisión.

Para asegurar estos y otros puntos de sus condiciones de uso, los usuarios deben de cumplir con las normas comunitarias de Instagram, cuyo objetivo es respetar la diversidad de culturas, edades y creencias.

---

[137] Obtenido de la Política relativa al contenido multimedia de Twitter disponible en: *https://help.twitter.com/es/rules-and-policies/media-policy*

[138] Disponibles para su consulta en *https://help.instagram.com/478745558852511*

Respecto de la política de privacidad, debe recordarse que en 2012 fue absorbido por Facebook, de tal manera que, con independencia de ese hecho, los usuarios deben de ajustarse a las condiciones establecidas en ambas plataformas.

Dentro de la información que se recopila se encuentra la relativa al nombre de usuario, contraseña y dirección de correo electrónico al registrarte en una cuenta de Instagram; la información que compone el perfil de usuario, aquella que derive del contenido de usuario como fotos, comentarios y otros materiales, así como los contactos que usen esta red social o aquellos que se les pueda invitarlos a su participación.

También establece que es posible compartir el contenido del usuario e información procedente de cookies, archivos de registro, identificadores de dispositivo, datos de ubicación y datos de uso con empresas que formen parte legalmente del mismo grupo de empresas al que pertenece Instagram ("Filiales"), mismas que pueden utilizar esta información para ayudar a proporcionar, entender y mejorar el Servicio y los servicios propios de las Filiales.

En cuanto al uso de información de menores de 14 años de edad, Instagram prohíbe el registro de los mismos, ya que el servicio y su contenido no están destinados a este sector de la sociedad; de tal manera que, en los casos que se detecte información personal de menores de 14 años sin autorización paterna, se borrará esa información lo más rápido posible o en su caso, permite denunciar la cuenta[139] si se considera que corresponde a un menor de 14 años o a información de éste.

Snapchat

Esta clase de red social permite el envío de imágenes o videos de forma individual o grupal y una vez entregada, estará disponible para el receptor de 1 a 10

[139] El procedimiento es muy sencillo y se puede localizar en el siguiente vínculo electrónico, en el que únicamente resulta necesario el nombre de usuario de la cuenta, el nombre de la persona denunciada, la fecha de nacimiento de la persona y la relación con dicha persona, es decir si se es familiar o se relaciona por otro motivo: *https://help.instagram.com/contact/723586364339719?helpref=faq_content*

segundos, para su posterior eliminación. Por la naturaleza de esta red social, desde su lanzamiento tuvo una participación mayor por menores de edad.

Así las cosas, las condiciones de uso[140] de esta red social establece que ninguna persona menor de 13 años tiene permitido crear una cuenta o usar los servicios correspondientes a Snapchat y si bien cuenta con condiciones de uso aplicables a usuarios que residen dentro y fuera de Estados Unidos tal y como lo hace Twitter, a diferencia de la última, el límite de edad se encuentra en ambas versiones.

De acuerdo con la política de privacidad de Snapchat[141], se encuentra redactada en términos comunes, de tal manera que resulta más comprensible el contenido de la totalidad del documento, además de establecer que se encuentran adheridos al Escudo de la privacidad de Estados Unidos y Suiza.

La información que recaba se divide en la que comparte el usuario con Snapchat (nombre de usuario, contraseña, dirección de correo electrónico, un número de teléfono, fecha de nacimiento, imágenes de perfil, u otra información útil de identificación). Y para algunos productos comerciales se puede requerir el número de una tarjeta de débito o de crédito y la información de la cuenta correspondiente; la que se recaba en el uso de los servicios que presta (sobre la actividad a través de nuestros servicios, como los nombres de los usuarios, la hora y fecha de las comunicaciones, el número de mensajes que se intercambian y las interacciones con los mensajes, por ejemplo cuando se abre un mensaje o hace una captura de pantalla), entre otros datos.

En cuanto a la que se obtiene de terceros, consiste en aquella, que otro usuario otorga mediante el acceso a datos de la agenda de contactos de su dispositivo, de tal manera que se combine esa información con otra que se recabe sobre el usuario; también se obtiene información de sus filiales, o cualquier otra fuente externa, y combinarla con la que recaban a través de sus servicios.

---

[140] Disponible para su consulta en *https://www.snap.com/es/terms/#terms-row*

[141] Disponible para su consulta en *https://www.snap.com/es/privacy/privacy-policy/*

Aunado a lo anterior, recalca que sus servicios no están diseñados ni se encuentran dirigidos a menores de 13 años, por lo que no recaban a sabiendas información personal de ninguna persona menor de 13 años, y en cuyo caso permite a los demás usuarios denunciar esta clase de incumplimiento de sus condiciones de uso.

Tumblr

Es una red social que permite a los usuarios seguir a otros a través de *blogs* o publicaciones, incluyendo textos, imágenes, mensajería instantánea, audio y video, que permiten ser editados por los demás miembros de Tumblr.

Un dato interesante consiste en que, si bien la cantidad de usuarios de esta red social puede abarcar múltiples lugares a nivel mundial, sus condiciones de uso y las políticas de privacidad se encuentran redactadas únicamente en inglés ya que "Tumblr es una empresa estadounidense y solo está sujeta a la legislación y jurisdicción de EE. UU."[142] (sic).

En dichas condiciones de uso, se establece que para formar parte de esta red social se debe ser mayor a los 13 años de edad, conforme a la legislación federal y estatal de los Estados Unidos; sin embargo, no se advierte algún procedimiento para eliminar contenido correspondiente a personas menores a dicha edad.

En cuanto al contenido que recopila de los usuarios, establece de manera enunciativa más no limitativa que recopila el nombre, dirección, número telefónico, dirección de correo electrónico y cualquier otro que derive de las publicaciones que se realicen en la red social, de tal manera que se replican los usos que las demás redes sociales utilizan de sus usuarios; es decir, el uso de dicha información con el fin de mejorar los servicios, la experiencia o cualquier otro uso que derive de los contenidos que en ella se concentren.

Por lo anterior, resulta claro que no existe uniformidad entre la edad mínima para ser usuarios de redes sociales o cualquier otra clase de aplicaciones, tampoco

---

142 Obtenido de: *https://www.tumblr.com/policy/en/terms-of-service* y *https://www.tumblr.com/policy/en/privacy*.

para la estructura o puntos mínimos de las políticas de privacidad y las condiciones de uso.

Además de las redes sociales indicadas, aplicaciones de servicio de mensajería como WhastApp[143], establecen que la edad mínima para acceder a los servicios de la misma es de 13 años; en cambio, aplicaciones cuyo objetivo comercial son adolescentes y adultos, establecen otras edades como mínimas para acceder a sus servicios, tal es el caso de LinkedIn cuya edad mínima es de 16 años[144], o Tinder que establece el mínimo de 18 años para acceder a dicha aplicación.

Cada desarrollador cuenta con la capacidad de decidir el mínimo de edad correspondiente para acceder a los servicios que brinde su aplicación o red social; sin embargo, debe siempre de garantizar la protección de datos personales de sus usuarios a través de políticas de privacidad acordes a la normativa aplicable y en su caso, proteger con mayores estándares los datos personales de menores de edad.

3.2. Recomendaciones

Por lo anteriormente indicado, en el caso específico de los menores, el acceso a las redes sociales debe darse con el acompañamiento de los padres o personas responsables de su cuidado, a fin de que éstos sean conscientes de que si bien el mundo de la información y la tecnología implica una infinidad de beneficios para su desarrollo, al mismo tiempo genera una serie de riesgos que se pueden evitar con un correcto manejo de la información y con una adecuada interacción con los demás miembros de la red.

---

143 Conforme a sus condiciones de uso, disponibles en: *https://www.whatsapp.com/legal/?l=es*

144 Conforme a sus condiciones de uso, disponibles en: *https://www.linkedin.com/legal/user-agreement?_l=es_ES*

Tales riesgos pueden ser evitados si se tiene conocimiento acerca del funcionamiento y las políticas de privacidad de los diferentes sitios en línea, en especial de las redes sociales.

De tal manera que, al ser el interés superior del menor lo que debe prevalecer, como derecho humano, y si los niños que se convierten en adolescentes, se conjuntan en una red social conformada por sus amigos, compañeros y, en su caso, familiares, se vuelve peculiarmente, uno de los principales círculos de convivencia entre ellos en el que el tipo de contenido compartido refleja la pertenencia a las diversas redes sociales que utilizan.

La exposición (entendido como una representación pública) de los datos personales de menores, mientras usan redes sociales en Internet o en su caso la publicación de los mismos hecha por cualquier persona, a través de computadoras o dispositivos móviles, en la mayoría de los casos se lleva a cabo sin tener cuidado o conocimiento de la responsabilidad que implica este hecho, ya que puede aumentar el riesgo de sufrir algún menoscabo en los derechos de los menores de edad.

Cada día crece esta “necesidad” de compartir información con terceros en Internet, por parte de los padres o tutores desde que los menores de edad son bebés y que cubren cada aspecto de la vida cotidiana, incluyendo los momentos más privados en su familia y con su círculo de amigos.

Las consecuencias de estos hechos, dentro y fuera de las redes sociales, implican diversos peligros para los menores de edad, dentro de los cuales se localizan los fines para los que su información puede ser utilizada, y que, en el peor de los casos, los padres o tutores son los últimos en identificar.

Por tanto, es necesario generar recomendaciones que capaciten a los usuarios, en este caso menores de edad y demás actores involucrados, respecto del correcto uso y en su caso transmisión de información dentro de las redes sociales en Internet.

Por lo anterior, a continuación, se identifican algunas recomendaciones para la protección de datos personales de menores en redes sociales, especificando que son sólo enunciativas y no limitativas:

Respecto de los padres con sus hijos o de sus tutores:

1. Antes de generar alguna mala impresión respecto del uso de redes sociales y los prejuicios que existen por el mismo, resulta de toral importancia tener un acercamiento por parte de los padres o tutores al uso de la tecnología y conocer por su cuenta las características que tiene el uso de datos personales en cualquier red social que sea de su interés.

Lo anterior, con el fin de poder promover día con día la protección de datos personales de sus hijos, y en su caso, prever la actualización de cualquier riesgo que los padres o tutores hayan identificado en su experiencia dentro de la red de redes.

2. Resulta fundamental prestar atención meticulosa al contenido que suben los hijos a las redes sociales, ya que resulta factible que pueda ser copiado y guardado por cualquiera, este riesgo aumenta por la cantidad de pornógrafos infantiles que se encuentran en redes sociales y otros sitios.

Para lograr lo anterior, existen diversas alternativas que permiten conocer qué información se coloca en los perfiles de sus hijos y a su vez, aumentar el nivel de protección de sus datos personales en la red de redes, mismas que a continuación se indican:

3. Ajustar los niveles de privacidad del perfil del menor dentro de las redes sociales a la que pertenezca, limitando el acceso a su información de parte de determinadas personas (ajenas en cualquier círculo social del menor), de tal manera que no afecten su desarrollo íntegro, privilegiando el interés superior del menor en todo momento.

Por ejemplo, evitar que cualquier persona desconocida pueda agregar a sus hijos o que permita interactuar con ellos, a través de los medios de comunicación que forman parte de la red social, como los mensajes internos o publicaciones sin restricciones de cualquier tipo de interacción, como comentarios o calificaciones (los denominados “me gusta”).

4. Verificar continuamente los contactos con los que el menor puede tener acceso en la red social, principalmente con una amplia comunicación entre él y sus padres o tutores.

Es decir, conocer a las personas con las que sus hijos mantienen contacto ya sea dentro de la red social o en el mundo físico, partiendo de los círculos sociales a los que pertenece. Con lo dicho, el padre de familia puede involucrarse de mejor manera sin invadir la privacidad del menor, ya que le permite identificar qué personas tienen contacto con sus hijos y en su caso, la identificación de cualquier persona que pudiese afectar su esfera jurídica.

En este caso los padres o tutores tienen la oportunidad de identificar junto con sus hijos el perfil de los usuarios que interactúan en la misma red social y en su caso, identificar relaciones que pudiesen ser dañinas o riesgosas para el menor de edad.

5. En caso de tener una foto de perfil del menor, elegir una en que no lo coloque en una situación vulnerable frente a probables actos de discriminación, Ciberbullying, pornografía infantil, entre otras situaciones desfavorables para el menor, ya que las fotos inapropiadas pueden llamar la atención de personas equivocadas, con intenciones peligrosas o lesivas.

Respecto de este punto, los padres de familia pueden acercarse a sus hijos en cuanto al correcto uso de su imagen en Internet, y al mismo tiempo, les permite aumentar la comunicación con sus hijos en caso de presentarse alguna situación que afecte al niño, niña o adolescente.

6. Dentro de la configuración de privacidad del perfil de menor, hacer las modificaciones correspondientes respecto de las personas que pueden identificar o etiquetar dentro de las redes sociales al menor en las fotografías que en éstas se agregan.

Lo anterior permite que el menor procure tener un control de las imágenes que lo involucran, así como de las demás interacciones que se generen por alguna publicación que se relacione con él.

Cabe señalar que son diversas redes sociales las que permiten al usuario aceptar o rechazar la identificación o etiqueta que realice un tercero, respecto de su propia imagen, previo a la aparición en su perfil e incluso tiene la posibilidad de eliminar o denunciar la publicación por considerar que podría afectarlo de cualquier manera.

7. Comunicación permanente con el menor sobre qué hacer y qué no, al momento de subir cualquier clase de información a Internet, específicamente cuando se trata de datos personales.

Un claro ejemplo de estos casos, se presenta en el momento en el que el menor de edad pretende publicar su fecha de nacimiento, nombre completo, dirección, teléfono, escuela en la que estudia, o cualquier otro dato personal que no resulte necesario compartir en redes sociales.

En estos casos, los padres de familia podrían identificar en compañía de sus hijos la importancia que tiene el resguardo y cuidado de información personal, a la que sólo determinadas podrían acceder, así como la explicación del deber de cuidado que deben de tener respecto de dichos datos en Internet y en el mundo físico.

Respecto de los padres o tutores.

8. Valorar la necesidad de subir fotos de la vida de los menores en las redes sociales, ya que es necesario definir los alcances que tiene esa publicación en el futuro.

Es decir, si bien en la actualidad resulta importante para algunos padres hacer pública la vida de sus hijos, a partir de la publicación de fotos, videos, calificaciones, rutas o cualquier otra información que involucre el que hacer de sus hijos, se debe tener en claro que toda vez que se realiza esta publicación sin el consentimiento del menor, el padre o la persona que la lleva a cabo debe recordar en todo momento que frente a cualquier acción, se debe de respetar el interés superior del menor.

Además, en cuanto al alcance de la publicación, se debe recordar que una vez que cualquier dato ingresa a Internet, es sumamente complicado lograr la eliminación de toda la información que derive de la misma, siendo así que la madre o padre que desee publicar información personal de sus hijos, debe ponderar si prefiere obtener un “me gusta”, “retweet” o comentario a cambio de la exposición de sus hijos en redes sociales.

También deben conocer que la información que se encuentra en Internet difícilmente podrán eliminarlas, y en muchos casos no es posible desindexarlas de los datos correspondientes a los menores de edad.

9. Si se decide publicar y compartir fotografías, videos o cualquier otro dato personal de menores de edad, resulta conveniente solicitar a las personas que pueden acceder a dicha información que sean discretos al momento de visualizarla y en su caso, abstenerse de compartirla con terceros.

De igual forma, uno debe ser precavido en los momentos que, por cualquier motivo, recaba más datos personales de los que quisiera, por ejemplo, en una fiesta de cumpleaños, una salida al parque, vacaciones o algún festival en la escuela, por lo que antes de la publicación de la foto o video resulta coherente pedir el permiso o autorización correspondiente a los padres de los niños que en ellos aparecen.

10. Evitar la publicación de información que en un futuro pueda considerarse motivo de pena o vergüenza para el menor de edad, ya que, si no se toman las precauciones correspondientes, pueden sufrir cualquier clase de maltrato o abuso, dentro y fuera de Internet.
11. Reconocer que, si bien las publicaciones que se realicen en Internet de los menores de edad, pueden estar limitadas a algún círculo de contactos, éstos podrían compartir con otras personas los mismos contenidos que aparentemente eran exclusivos y limitados para su consulta.

Resulta indispensable que los padres de familia tomen las medidas de precaución necesarias para lograr nulificar cualquier riesgo o daño a los datos personales de menores de edad, tales como difuminar cualquier rasgo o detalle que los identifique, editar los datos que permitan identificar su ubicación u lugares que frecuenta, entre otras acciones.

Esto va de la mano con la cultura de la protección de los datos personales y de la intimidad, que pueden enseñar los mayores a los niños, niñas y adolescentes, de tal manera que recuerden en todo momento que deben proteger esos ámbitos de su vida, cuyo nivel de protección es superior debido a la naturaleza de información que de ellos desprende.

12. Iniciar con el ejemplo, es decir, como padres o responsables de menores, no es congruente solicitar mayores precauciones a los menores, cuando los adultos no las emplean en su vida cotidiana.

Los niños son capaces de simular o replicar los actos que identifican de sus mayores, por lo que los padres de familia o tutores deben de tener en cuenta que, en cualquier momento, sus hijos podrían realizar el mismo tipo de publicaciones que ellos realizan y por las que se expongan a riesgos innecesarios.

13. En el caso de información que requiera una mayor protección, como lo son los datos personales sensibles, transmitir dicha información de un equipo a otro por medios que no involucren su carga a Internet, y de no ser posible, llevarlo a cabo por medios encriptados, los cuales disminuyen el riesgo de una vulneración a su seguridad, toda vez que si se publican en una red social se está compartiendo con diversos contactos (amigos, compañeros del trabajo, excompañeros de la escuela, etcétera) y que respecto de la publicación, nunca se podrá identificar plenamente qué pueden llegar a hacer con esa foto.

14. En cuanto a la navegación de cualquier usuario de Internet en el hogar, contar con mecanismos de seguridad que procuren proteger la información de los dispositivos que acceden a la red de redes, tales como antivirus, firewall y antispam.

15. Los padres y tutores deben aceptar que resulta necesario conocer de mejor manera el funcionamiento de las redes sociales, de los dispositivos electrónicos, del Internet en sí mismo, y de aquellas conductas que se van presentando día con día y que pudiesen representar algún riesgo para sus hijos o pupilos.

Prácticamente, consiste en educarse en este nuevo ámbito digital aparentemente desconocido para ellos, pero tan familiar para los menores de edad, de tal forma que sea incluso un tema en común entre padres e hijos que les permita conocerse más y lograr un alto nivel de confianza en su relación.

16. Lo anteriormente señalado da cuenta de los riesgos y problemas a los que están expuestos los datos personales que publicamos en redes sociales, sin tener pleno conocimiento sobre el perjuicio que se puede generar en nuestra vida privada, lo cual entra en una ponderación frente al costo, que en la mayoría de los casos es nulo, y el beneficio que implica formar parte de diversas redes sociales teniendo acceso a diversos servicios a cambio de entregar una cantidad infinita de datos personales.

Frente a este problema, podrán generarse múltiples medidas preventivas hacia un control del uso de nuestros datos personales. Por ejemplo, Heidy Balanta [145] propone que debemos tener en cuenta cuatro puntos previos a la publicación de datos personales, que son los siguientes:

1) Saber a quién se entregan los datos personales.
2) Identificar plenamente qué información se entrega.
3) Tener en cuenta que los datos que se entrega nunca se los devolverán, por lo que hay que ser precavido con la información que se transmite.
4) Recordar que nada es privado en Internet por lo que cualquier cosa que envíe, comparta, transfiera o almacene, algún tercero podría estar viéndolo.

Respecto de los creadores o administradores de redes sociales (industria).

17. Si bien el desarrollo de redes sociales puede resultar ser un gran negocio por la gran cantidad de anuncios que se presentan en la navegación de sus usuarios en Internet, así como por el uso de datos personales que logran administrar, resulta importante que, en el diseño y desarrollo de la red social, se cumplan con los estándares de seguridad internacionales respecto del tratamiento de datos personales, junto con los principios y deberes en la materia.

---

[145] Balanta, Heidy, *Sus datos personales tienen un valor económico: ¿está ganando o perdiendo?,* Derecho Informático, marzo de 2014, http://derechoinformatico.co/sus-datos-personales-tienen-un-valor-economico-esta-ganando-o-perdiendo/

Si bien este punto, puede resultar más complejo en cuanto a su cumplimiento, es dable presumir que, ante un estándar de seguridad internacional respecto del uso de datos personales, aumenta el valor de la red social y el número de usuarios que deseen utilizarla.

Un ejemplo del efecto social que puede tener este hecho se refleja en las pérdidas millonarias que han tenido empresas como Sony o Apple cuando se publican filtraciones de la base de datos de dichas empresas o fallas en sus sistemas de seguridad.

18. En el diseño de las redes sociales, procurar actuar de la manera más ética.

Toda vez que los usuarios confían en los servicios que se encuentran a su disposición en Internet, se debe de tomar en cuenta que los desarrolladores de las redes sociales podrían respetar entre otras cosas, los datos personales de sus usuarios y si dentro de su negocio es necesario hacer alguna operación que los involucre, se cumpla con la normativa aplicable a su tratamiento y, por tanto, se le informe de dicha situación a sus usuarios.

Un mecanismo para lograr este objetivo es palpable a través de la adopción de códigos de ética por sector, en el que se garantice el derecho de protección de datos personales, frente a sus clientes o cualquier miembro de la sociedad, en colaboración con el organismo garante correspondiente, a fin de cumplir con el marco jurídico.

19. En la elaboración de las condiciones de privacidad o políticas de privacidad de cada red social, el desarrollador o administrador de la red social, podría diseñar de manera más simple e igual de informada los términos y condiciones a los que se sujetan las personas que deseen acceder a sus servicios.

De esta manera, los usuarios podrán conocer de manera completa e informada cada una de las condiciones que involucran el tratamiento de sus datos personales, mediante palabras más simples, o incluso a través de dibujos que permitan identificar a cada usuario, las características de su red social y todo lo que su uso implica.

20. Diseñar un módulo o sección dentro de la red social dirigido a menores de edad, en el cual se le haga de su conocimiento cada uno de los riesgos que podrían localizar en Internet, así como los mecanismos con los que cuentan para denunciar conductas que pudiesen afectarlo.
21. Establecer la posibilidad de que el usuario pueda elegir en qué y cómo serán utilizados sus datos personales, informando en todo momento la manera en que tales decisiones podrían afectar la experiencia de navegación o interacción dentro de la red social.
22. Ajustar los mecanismos, formatos o herramientas de la red social para que sean afines a la privacidad por diseño, evitando la recopilación de información innecesaria, evitando así ser responsable de más datos personales de los estrictamente útiles para el usuario y el administrador.
23. Conseguir certificaciones o sellos de empresas digitalmente responsable correspondientes al derecho de la protección de datos personales, lo cual permitiría demostrar a sus clientes o usuarios, el respeto a su privacidad conforma la normativa y estándares vigentes, así como su actualización constante.
24. Aunado a lo anterior, se sugiere la implementación de una figura similar al defensor de audiencias contenido en la Ley Federal de Telecomunicaciones, pero en el caso de redes sociales tendría la función de mantener contacto directo con sus usuarios, en el que se permita intercambiar inquietudes o resolver problemáticas relacionadas con el tratamiento de sus datos personales, lo cual permitiría abrir un canal de comunicación directo en el que sea acorde a su política de privacidad y a la legislación vigente en la materia.

Respecto del Estado

25. Emitir marco jurídico idóneo a estándares internacionales, de tal manera que no se dificulte el ejercicio de derechos ARCO por parte de los menores de edad, con responsables dentro del territorio mexicano y con aquellos que lleven a cabo tratamiento de datos personales fuera del país.

26. Desarrollar e implementar políticas públicas que prevengan la salvaguarda del derecho de protección de datos personales de niños, niñas y adolescentes, en Internet, con especial atención al caso de las redes sociales, provocando que con estas acciones se garantice el efectivo cumplimiento de ese derecho fundamental
27. Promover a través de su competencia que, por medio del avance tecnológico junto con la ciencia, el enfoque que se tiene respecto de la protección de datos personales cambió hacia la necesidad de desplegar otros mecanismos de garantía, siendo un tema de toral importancia el uso de las nuevas tecnologías, teniendo en cuenta que en sí mismas las TIC no son “malas” sino que lo es el uso que la gente le dé a las mismas, respecto de los datos personales.
28. Involucrarse en la promoción del derecho de cada ser humano a la protección de datos personales, ya que de esa manera podría actuar en dos vías, la primera por medio de los mecanismos normativos con los que cuente para garantizar este derecho y la segunda por la cultura de cuidado frente al uso de datos personales en Internet, específicamente en redes sociales.
29. Aunado a lo anterior, los diversos acuerdos, foros o convenios internacionales entre los Estados y organizaciones civiles podrían fomentar el desarrollo de posibles soluciones a esta clase de problemas tecnológicos, que continúe con la transformación cultural hacia una sociedad del conocimiento que permita utilizar las TIC, protegiendo en todo momento sus datos y vida privada en las redes sociales.
30. Actualizar a su personal en temas relacionados con el uso de datos personales y las TIC, de manera que se mejore el nivel de atención a los procedimientos que inicien los particulares respecto de la protección de su información en redes sociales.
31. Emitir mecanismos o herramientas que les permitan a los ciudadanos ejercer el derecho de protección de datos personales de manera efectiva y sin obstáculos dentro y fuera de Internet

32. Establecer mecanismos en los que la academia y la sociedad civil tengan voz y voto para el desarrollo de políticas afines a la protección de datos personales de menores en redes sociales.
33. Acercarse a las comunidades más desprotegidas, a las escuelas y a los padres de familia o tutores mediante pláticas, capacitaciones o cualquier otro mecanismo que les permite identificar de manera plena el valor de sus datos personales y los probables riesgos a los que se enfrentan diariamente en las redes sociales.

Bibliografía

Libros

ALEXY, Robert. "Derechos fundamentales ponderación y racionalidad", *Revista Iberoamericana de Derecho Procesal Constitucional*, México, 2009, núm. 11, enero-junio de 2009.

AMARO LÓPEZ, José Antonio, Chávez Aceves, Ch. y Varela Navarro, Gerardo Alberto, "La Web Oculta y cómo los buscadores encuentran la información", *Paakat: Revista de Tecnología y Sociedad*, año IV, núm. 7, septiembre 2014 - febrero 2015, *http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/221/326#referencias* (última fecha de consulta 3 de mayo de 2018).

BALANTA, Heidy, *Sus datos personales tienen un valor económico: ¿está ganando o perdiendo?,* Derecho Informático, marzo de 2014, http://derechoinformatico.co/sus-datos-personales-tienen-un-valor-economico-esta-ganando-o-perdiendo/ (última fecha de consulta 3 de mayo de 2018).

BOLDOVA, MIGUEL A, *Pornografía infantil en la red. Fundamento y límites de la intervención del Derecho Penal*, México, Ubijus, 2009

CÁRDENAS MIRANDA, Elva L, "El interés superior del niño", *Revista Letras Jurídicas*, México, 2011, Vol. 23, julio-diciembre 2010, *http://letrasjuridicas.com.mx/Volumenes/23/18a.pdf* (última fecha de consulta 3 de mayo de 2018).

CARRILLO, Miroslava*, "*Políticas públicas para proteger los datos personales de los menores en internet y en redes sociales*", Retos de la protección de dato personales en el sector público,* México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011*, http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf.* (última fecha de consulta 3 de mayo de 2018).

CENDOYA, Román, *Revolución del homo sapiens al homo digitalis*. Barcelona, Sekotia S. L. 2013

DEL RÍO, Jorge *et al*., "Menores y redes ¿sociales? De la amistad al cyberbullying". *Revista de estudios de juventud*, España, 2010, núm. 88,

http://www.injuve.es/sites/default/files/RJ88-09.pdf. (última fecha de consulta 3 de mayo de 2018).

FERNÁNDEZ SEGADO, Francisco (ed.), The Spanish Constitution in the European constitutional context. La Constitución española en el contexto constitucional europeo, Madrid, Dykinson, 2003, *http://www.corteidh.or.cr/tablas/r25294.pdf* (última fecha de consulta 3 de mayo de 2018).

GONZÁLEZ MARTÍN, Nuria y Rodríguez Benot, Andrés, (coords.), "Adopción Internacional", *Estudios sobre adopción internacional*, UNAM, Instituto de Investigaciones Jurídicas, México, 2001

GONZÁLEZ RODRÍGUEZ-ARNAÍZ, Graciano, "El imperativo tecnológico una alternativa desde el humanismo. cuadernos de bioética", *Revista Cuatrimestral de Investigación,* Madrid, año 2004, volumen XV, núm. 53. enero – abril, *http://aebioetica.org/revistas/2004/15/1/53/37.pdf* (última fecha de consulta 3 de mayo de 2018).

GONZÁLEZ, Graciano, "El imperativo tecnológico, una alternativa desde el humanismo", *Cuaderno Bioética* Madrid, Universidad Complutense de Madrid, 2004, *http://aebioetica.org/rtf/04bioetica53.pdf* (última fecha de consulta 3 de mayo de 2018).

GREGORIO, Carlos G., "Protección de datos personales: Europa vs Estados Unidos, todo un dilema para América Latina", en Hugo Cocha Cantú Hugo, Sergio López-Ayllón y Lucy Tacher Epelstein (coords.) *Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información*, México, UNAM, Instituto de Investigaciones Jurídicas, 2005, *https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf* (última fecha de consulta 3 de mayo de 2018).

GREGORIO, Carlos G. y Ornelas Lina (comps.) *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes*, Instituto de Investigación para la Justicia e Instituto Federal de Acceso a la Información y Protección de Datos, México, 2011, *http://libros.metabiblioteca.org/bitstream/001/307/9/978-968-5954-59-4.pdf* (última fecha de consulta 3 de mayo de 2018).

JIMÉNEZ GARCÍA, Joel Francisco, *Derechos de los niños*, México, Instituto de Investigaciones Jurídicas, 2000, *http://biblio.juridicas.unam.mx/libros/1/69/tc.pdf* (última fecha de consulta 3 de mayo de 2018).

MANZANERO FERNÁNDEZ, Delia María. "El Uso Virtuoso De La Tecnología", *Nómadas. Revista Crítica de Ciencias Sociales y Jurídicas*, Madrid, año 2007, núm. 15 (2007-1). *http://pendientedemigracion.ucm.es/info/nomadas/15/deliamanzanero.pdf* (última fecha de consulta 3 de mayo de 2018).

MARTÍNEZ, Ricard. "El derecho fundamental a la protección de datos: perspectivas.", *Revista de Internet, Derecho y Política,* España, III Congreso Internet, Derecho y Política, núm. 5, 2007, *https://dialnet.unirioja.es/descarga/articulo/2372613.pdf* (última fecha de consulta 3 de mayo de 2018).

MUÑOZ DE ALBA MEDRANO, Marcia, *Habeas Data*, México, UNAM, Instituto de Investigaciones Jurídicas, 2006, *http://biblio.juridicas.unam.mx/libros/5/2264/4.pdf* (última fecha de consulta 3 de mayo de 2018).

PULIDO JIMÉNEZ, Miguel, "Convergencias y divergencias: Acceso a la Información y la tutela de los datos personales", *Retos de la protección de dato personales en el sector público*. México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011, *http://www.infodf.org.mx/comsoc/campana/2012/LIbrodatosPweb.pdf* (última fecha de consulta 3 de mayo de 2018).

RAMÍREZ B., Edgar Roy, "Crítica al imperativo tecnológico", *Revista de Filosofía de la Universidad de Costa Rica*, Costa Rica, año 1998, volumen XXXVI, núm. 88/89, http://www.inif.ucr.ac.cr/recursos/docs/Revista%20de%20Filosof%C3%ADa%20UCR/Vol.%20XXXVI/No.88-89/Cr%C3%ADtica%20al%20imperativo%20tecnol%C3%B3gico.pdf (última fecha de consulta 3 de mayo de 2018).

RODRÍGUEZ, Gabriela et. al., *Interpretación conforme*. México, Comisión de Derechos Humanos del Distrito Federal - Suprema Corte de Justicia de la Nación - Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2013, *http://www2.scjn.gob.mx/red/coordinacion/archivos_Interpretacion.pdf* (última fecha de consulta 3 de mayo de 2018).

WARREN, Samuel D. y Brandeis, Louis D, “The Right To Privacy”, *Harvard Law Review*, Estados Unidos, 1890, Vol. IV, núm. 5, diciembre 1890, *http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf* (última fecha de consulta 3 de mayo de 2018).

Normativa nacional

Constitución Política de los Estados Unidos Mexicanos

Ley General de los Derechos de Niñas, Niños y Adolescentes

Ley General de Población

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Código Civil Federal

Código Penal para el Distrito Federal

Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Reglamento de la Ley General de Población

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, acuerdo número ACT-PUB/25/10/2016.06, *http://inicio.ifai.org.mx/AcuerdosDelPleno/ACT-PUB-25-10-2016.06.pdf* (última fecha de consulta 3 de mayo de 2018).

Normativa internacional

Código sobre la Protección de Datos Personales, *http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248* (última fecha de consulta 3 de mayo de 2018).

Convención Americana de Derechos Humanos, *https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm* (última fecha de consulta 3 de mayo de 2018).

Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia, *https://www.boe.es/boe/dias/2010/09/17/pdfs/BOE-A-2010-14221.pdf* (última fecha de consulta 3 de mayo de 2018).

Convención sobre los Derechos del Niño, *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CRC.aspx* (última fecha de consulta 3 de mayo de 2018).

Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento de Datos de Carácter Personal, *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf* (última fecha de consulta 3 de mayo de 2018).

Declaración de las Naciones Unidas sobre los Derechos del Niño, *https://www.oas.org/dil/esp/Declaraci%C3%B3n%20de%20los%20Derechos%20del%20Ni%C3%B1o%20Republica%20Dominicana.pdf* (última fecha de consulta 3 de mayo de 2018).

Declaración Universal de Derechos Humanos, *http://www.un.org/es/universal-declaration-human-rights/* (última fecha de consulta 3 de mayo de 2018).

Directiva 95/46/CE del parlamento europeo y del consejo de 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.

Ley N° 633 de 22 de abril de 1941 sobre la Protección del Derecho de Autor y los Derechos Conexos, *http://www.wipo.int/wipolex/es/text.jsp?file_id=301483* (última fecha de consulta 3 de mayo de 2018).

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes, *http://www.iijusticia.org/Memo.htm* última fecha de consulta 3 de mayo de 2018).

OC-17/2002 Corte Interamericana de Derechos Humanos, *http://www.corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf* (última fecha de consulta 3 de mayo de 2018).

Pacto Internacional de Derechos Civiles y Políticos, *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx* (última fecha de consulta 3 de mayo de 2018).

Pacto Internacional de Derechos Económicos, Sociales y Culturales, *http://www.ohchr.org/SP/ProfessionalInterest/Pages/CESCR.aspx* (última fecha de consulta 3 de mayo de 2018).

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril de 2016, *http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/reglamentos/common/pdfs/Reglamento_UE_2016-679_Proteccion_datos_DOUE.pdf* (última fecha de consulta 3 de mayo de 2018).

Red Iberoamericana de Protección de Datos, *Estándares de Protección de Datos Personales para los Estados Iberoamericanos,* junio 2017, *http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf* (última fecha de consulta 3 de mayo de 2018).

Resolución del grupo de trabajo Artículo 29 en materia de protección de datos en redes sociales (Dictamen 5/2009 sobre las redes sociales en línea).

Comunicados y notas periodísticas.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Carácter de dato personal de la dirección IP. Informe 327/2003*, España, 2003 *https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/otras_cuestiones/common/pdfs/2003-0327_Car-aa-cter-de-dato-personal-de-la-direcci-oo-n-IP.pdf* (última fecha de consulta 3 de mayo de 2018).

AMIGÓN, Edgar, "Robo de identidad, un delito en aumento", *Proteja su dinero,* México, CONDUSEF, núm. 186, septiembre 2015, *http://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf* (última fecha de consulta 3 de mayo de 2018).

BLASCO, Lucía, *Qué es el peligroso juego de "La ballena azul" y por qué preocupa a las autoridades,* BBC Mundo, publicado 26 abril 2017, *http://www.bbc.com/mundo/noticias-39721105* (última fecha de consulta 3 de mayo de 2018).

CAGNAZZO, Raffaella, *Austria, dieciocho años, denuncia a sus padres por fotos publicadas en Facebook*, 15 de septiembre de 2016, Corriere della Sera, *http://www.corriere.it/esteri/16_settembre_15/austria-diciottenne-denuncia-genitori-*

foto-postate-facebook-2ceb737a-7b46-11e6-ae27-bc43cc35ec72.shtml (última fecha de consulta 3 de mayo de 2018).

EDIZIONES, Portaltic, *Así combaten la pornografía infantil las principales redes sociales*, Portal TIC/Europa Press, 14 de marzo de 2017, *http://www.europapress.es/portaltic/socialmedia/noticia-asi-combaten-pornografia-infantil-principales-redes-sociales-20170314085947.html* (última fecha de consulta 3 de mayo de 2018).

EL PAÍS, *¿Qué dice la sentencia del Tribunal de la UE sobre protección de datos?*, Madrid, 6 de octubre de 2015, *http://internacional.elpais.com/internacional/2015/10/06/actualidad/1444134525_731477.html* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, Estadísticas a propósito del… Día del Niño (30 de abril), *http://www.inegi.org.mx/saladeprensa/aproposito/2017/ni%C3%B1o2017_Nal.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, Estadísticas a propósito del Día Internacional de la Niña (11 de octubre), *http://www.inegi.org.mx/saladeprensa/aproposito/2017/Nina2017_Nal.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, "Estadísticas a propósito del… Día Mundial de Internet (17 de mayo)", 15 de mayo de 2017, *http://www.inegi.org.mx/saladeprensa/aproposito/2017/internet2017_Nal.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado INAI/089/17, "*En México hay más de 60 millones de usuarios de redes sociales; INAI emite recomendaciones para su uso", http://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-089-17.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado INAI/136/17, "C*uidado*

con la información que compartes en redes sociales, advierte INAI", http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-136-17.pdf (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado INAI/235/17, "Emite INAI recomendaciones de seguridad para usuarios de redes sociales", *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-235-17.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado INAI/092/17, "Sincronizar app's con redes sociales, riesgoso para la protección de datos personales", *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-092-17.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Comunicado INAI/229/17, "Advierte INAI riesgos de sincronizar app's con redes sociales y la forma de prevenirlos", *http://inicio.ifai.org.mx/Comunicados/Comunicado%20INAI-229-17.pdf* (última fecha de consulta 3 de mayo de 2018).

MONTALTO, Lillo, *Sentenciada a pagar 10 mil euros a su hijo si publica fotos suyas en Facebook*, *Euronews,* Italia, 9 de enero de 2018, http://es.euronews.com/2018/01/09/sentenciada-a-pagar-10-mil-euros-a-su-hijo-si-publica-fotos-suyas-en-facebook (última fecha de consulta 3 de mayo de 2018).

PROCURADURÍA FEDERAL DEL CONSUMIDOR, boletín de prensa 0058 *PROFECO y CONDUSEF firman convenio de colaboración en beneficio de consumidores y usuarios de servicios financieros*, 7 de junio de 2016, https://www.profeco.gob.mx/prensa/prensa16/junio16/bol00058.php (última fecha de consulta 3 de mayo de 2018).

SPUTNIK NEWS, *Una estudiante de 18 años de Carintia, Austria, ha demandado a sus padres por… subir sus fotos a Facebook sin su consentimiento*, Sputnik News, 20 de septiembre de 2016,

https://mundo.sputniknews.com/sociedad/201609201063569194-austria-carintia-facebook-privacidad/ (última fecha de consulta 3 de mayo de 2018).

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, Boletín UNAM-DGCS-335 *Existen en México tres grupos de familias con 11 variantes: estudio de la UNAM.* Publicado el 15 de mayo de 2017 en *http://www.dgcs.unam.mx/boletin/bdboletin/2017_335.html* (última fecha de consulta 3 de mayo de 2018).

Sitios y documentos electrónicos.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Conoce la Agencia, *http://www.agpd.es/portalwebAGPD/LaAgencia/informacion_institucional/conoce/index-ides-idphp.php* (última fecha de consulta 3 de mayo de 2018).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía sobre el uso de las cookies*, España, 2013, *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_Cookies.pdf* (última fecha de consulta 3 de mayo de 2018).

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS Y ASOCIACIÓN ESPAÑOLA PARA EL FOMENTO DE LA SEGURIDAD DE LA INFORMACIÓN, ISMS Forum Spain, *Código de buenas prácticas en protección de datos para proyectos big data*, España, 2017, *https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/Guia_Big_Data_AEPD-ISMS_Forum.pdf* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, Centro de seguridad, *https://www.facebook.com/help/safety* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, Latest Community Stats, *https://investor.fb.com/home/default.aspx* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, Política de datos completa, *https://www.facebook.com/full_data_use_policy* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, Política de datos, *https://www.facebook.com/about/privacy* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Cookies y otras tecnologías de almacenamiento*, *https://www.facebook.com/policies/cookies/* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Condiciones del servicio*, *https://www.facebook.com/legal/terms/update* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Centro de prevención del bullying*, *https://www.facebook.com/safety/bullying* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, Servicio de ayuda, *https://www.facebook.com/help/1561485474074139* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Portal para padres*, *https://www.facebook.com/safety/parents* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Cómo reportar contenido*, *https://www.facebook.com/help/181495968648557/?ref=sc* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Messenger Kids*, *https://messengerkids.com/* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Messenger Kids Terms of Service*, *https://www.facebook.com/help/1954771561401423* (última fecha de consulta 3 de mayo de 2018).

FACEBOOK, *Messenger Kids Privacy Policy*, *https://www.facebook.com/help/118909212153483* (última fecha de consulta 3 de mayo de 2018).

FLORES, Jorge. *Sexting: adolescentes, sexo y teléfonos móviles*. Pantallas Amigas, 2009. *http://www.pantallasamigas.net/proteccion-infancia-consejos-articulos/sexting-adolescentes-sexo-y-telefonos-moviles.shtm* (última fecha de consulta 3 de mayo de 2018).

INSTAGRAM, *Condiciones de uso, https://help.instagram.com/478745558852511* (última fecha de consulta 3 de mayo de 2018).

INSTAGRAM, *Denunciar a un usuario menor de edad en Instagram, https://help.instagram.com/contact/723586364339719?helpref=faq_content* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN DE ESPAÑA, el Observatorio de la Seguridad de la Información y PantallasAmigas, febrero de 2011, *http://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Convenio de colaboración entre el INAI y la CONDUSEF, *http://inicio.ifai.org.mx/ConveniosInstDocs/CONV-40-2016%20Procuraduria%20Federal%20del%20Consumidor%20PROFECO.pdf.* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Misión Visión y Objetivos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *http://inicio.inai.org.mx/SitePages/misionViosionObjetivos.aspx* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para prevenir el robo de identidad,* *http://inicio.inai.org.mx/DocumentosdeInteres/Gu%C3%ADa_Prevenir_RI.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, Convocatoria del Premio de Innovación y Buenas Prácticas en la Protección de Datos Personales 2017 del INAI, *http://premioinnovacionpdp.inai.org.mx/Pages/Convocatoria-y-bases.aspx* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL ELECTORAL, *Credencial [no solo] Para Votar Implementación de buenas prácticas en materia de Datos Personales en el Registro Federal de Electores,* 2016, *http://premioinnovacionpdp2016.inai.org.mx/Ganadores/Folio%2032%20INE.pdf* (última fecha de consulta 3 de mayo de 2018).

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN DE ESPAÑA, *Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y e-confianza de sus padres,* España, 2009, *http://www.pantallasamigas.net/actualidad-pantallasamigas/pdf/inteco-estudio-uso-seguro-tic-menores.pdf* (última fecha de consulta 3 de mayo de 2018).

LINKEDIN*, Condiciones de uso, https://www.linkedin.com/legal/user-agreement?_l=es_ES* (última fecha de consulta 3 de mayo de 2018).

MICROSOFT, *Descripción de las Cookies, https://support.microsoft.com/es-es/help/260971/description-of-cookies* (última fecha de consulta 3 de mayo de 2018).

MONSTRUOS EN RED, *https://www.youtube.com/watch?v=7xyCGCwKePM&list=PL1vMhg3AawgTfbsZ6zsOiDjwZ5VleQ4u9* (última fecha de consulta 3 de mayo de 2018).

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN, "*About ISO*", *https://www.iso.org/about-us.html* (última fecha de consulta 3 de mayo de 2018).

ORGANIZACIÓN INTERNACIONAL PARA LA ESTANDARIZACIÓN, "*ISO in brief*", *https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/isoinbrief_2015.pdf* (última fecha de consulta 3 de mayo de 2018).

ORGANIZACIÓN DE LAS NACIONES UNIDAS, *La población mundial aumentará en 1.000 millones para 2030,* 21 de junio 2017, *https://www.un.org/development/desa/es/news/population/world-population-prospects-2017.html* (última fecha de consulta 3 de mayo de 2018).

PANTALLASAMIGAS, *Grooming*, *http://internet-grooming.net/* (última fecha de consulta 3 de mayo de 2018).

SNAPCHAT, *Condiciones de servicio de Snap Inc., https://www.snap.com/es/terms/#terms-row* (última fecha de consulta 3 de mayo de 2018).

SNAPCHAT, *Política de privacidad, https://www.snap.com/es/privacy/privacy-policy/* (última fecha de consulta 3 de mayo de 2018).

TUMBLR, *Terms of Service, https://www.tumblr.com/policy/en/terms-of-service* (última fecha de consulta 3 de mayo de 2018).

TUMBLR, *Política de privacidad internacional de Tumblr, https://www.tumblr.com/privacy* (última fecha de consulta 3 de mayo de 2018).

TWITTER, *Reglas de Twitter*, *https://help.twitter.com/es/rules-and-policies/twitter-rules* (última fecha de consulta 3 de mayo de 2018).

TWITTER, *Twitter Terms of Service*, *https://twitter.com/tos?lang=en* (última fecha de consulta 3 de mayo de 2018).

TWITTER, *Twitter Términos de servicio*, *https://twitter.com/es/tos#updateintlWho* (última fecha de consulta 3 de mayo de 2018).

TWITTER, *Política relativa al contenido multimedia de Twitter*, *https://help.twitter.com/es/rules-and-policies/media-policy* (última fecha de consulta 3 de mayo de 2018).

WHATSAPP, *Información legal de WhatsApp, https://www.whatsapp.com/legal/?l=es* (última fecha de consulta 3 de mayo de 2018).

SLVCI, S.A. DE C.V., *Sistema de Control de Visitantes*, agosto 2016, México, *http://premioinnovacionpdp2016.inai.org.mx/Ganadores/Folio%2022%20SLVCI.pdf* (última fecha de consulta 3 de mayo de 2018).

SYMANTEC, ¿Cuánto cuestan los datos robados y servicios de ataque en el mercado clandestino?, *http://www.symantec.com/connect/blogs/cuanto-cuestan-los-datos-robados-y-servicios-de-ataque-en-el-mercado-clandestino* (última fecha de consulta 3 de mayo de 2018).

Jurisprudencia y precedentes

Corte Constitucional de la República de Colombia, Sentencia T-260/12 emitida por la Sala Octava de Revisión, 29 de marzo de 2012, *http://www.corteconstitucional.gov.co/relatoria/2012/T-260-12.HTM* (última fecha de consulta 3 de mayo de 2018).

Tesis 2a. VI/2018 (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 50, Tomo I, enero de 2018, p. 537.

Tesis. 1a. XIII/2012, Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro V, febrero de 2012, Pág. 650.

Tesis I.4o.A.20 K Semanario Judicial de la Federación y su Gaceta, Décima Época, Libro 1, diciembre de 2013, pág. 1211.

Tribunal de Justicia (Gran Sala) de la Unión Europea, Sentencia C-362/14, 6 de octubre de 2015, *http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES* (última fecha de consulta 3 de mayo de 2018).

Tribunal de Roma, Sentencia del expediente 39913/2015, 23 de diciembre de 2017 *http://www.altalex.com/~/media/altalex/allegati/2018/allegati%20free/tribunale_roma_ordinanza_23_dicembre_2017%20pdf.pdf* (última fecha de consulta 3 de mayo de 2018)