UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Facultad de Ciencias Políticas y Sociales

El desafío de la protección de datos en el ámbito de las redes sociales: el caso mexicano

TESIS

Que para obtener el título de

Licenciada en Ciencias Políticas y Administración Pública

PRESENTA

Pamela Hernández Martínez

ASESORA

Dra. Rosa María Lince Campillo

Ciudad Universitaria, CD.MX., 2020

Dedico esta tesis a aquella niña que vive dentro de mí, quiero que sepa que su sueño está por cumplirse y que será sólo el inicio de muchos más.

Agradecimientos

Gracias a Dios por permitirme vivir sana para cumplir con este sueño.

Gracias a mi madre y padre por su amor, comprensión, apoyo, fuerza, ánimos y consejos que me han impulsado a ser lo que soy.

Gracias a mi familia y su amor incondicional, por ser unos de los mayores móviles que me dan fuerza para continuar.

Agradezco de manera especial a todas aquellas personas, que si algún día leen esta hoja sabrán a quienes me refiero, que siempre me motivaron a continuar, me alentaron en los momentos más cruciales e hicieron que creyera en mí y en la culminación de esta tesis.

A la Dra. Lince, por su incondicional apoyo, entusiasmo y compromiso, porque sin su profesionalismo, entrega y gran corazón no hubiera podido comenzar ni concluir este proyecto.

A mi amiga Fernanda, gracias porque fuiste el ángel que Dios puso en mi camino para levantarme y recordarme que era capaz de estos y más.

ÍNDICE

INTRODUCCIÓN 5

CAPÍTULO 1. MARCO TEÓRICO DE LA PROTECCIÓN DE DATOS PERSONALES 10

1.1 ¿Qué son los datos personales? 10

1.2 Vida Privada, privacidad e intimidad 13

1.3 Derecho a la protección de datos personales 18

1.4 Derecho de datos personales como habilitador de otros derechos y libertades. 22

1.4 El derecho de protección de datos personales en México 24

1.5 Marco jurídico internacional del derecho a la protección de datos personales 32

1.6 Protección de datos personales y la evolución tecnológica 40

CAPÍTULO 2. EL NUEVO ESPACIO PÚBLICO DIGITAL: INTERNET Y LAS REDES SOCIALES 42

2.1 Internet 42

2.1.1 Evolución de la internet 46

2.2 Redes sociales 48

2.3 Datos personales en las redes sociales. 51

2.3.1 Redes sociales como fuente de exposición de datos personales y medio para tratar información personal. 52

2.3.2. Actores involucrados en el tratamiento de los datos personales en las redes sociales 59

2.3.3 Riesgos a la protección de datos personales en las redes sociales 63

2.4 Factores de riesgo atenuantes para delitos y prácticas ilícitas en redes sociales aunado a la disposición de datos personales en las redes sociales. 68

CAPÍTULO 3. PROTECCIÓN DE DATOS PERSONALES Y REDES SOCIALES EN MÉXICO 72

3.1 Alcance del uso de la internet y redes sociales en México. 72

3.2 Hábitos en materia de protección de datos personales en las redes sociales en México 75

3.2.1 Ejemplos de vulneración de datos personales en redes sociales en México.....82

3.3 Cultura de protección de datos personales en el espacio de interacción social de las redes sociales 87

3.4 Cultura de protección de datos personales en México.....89

3.4.1 Nivel de conocimiento sobre el derecho a la protección de datos personales en México.....89

CONCLUSIONES.....100

REFERENCIAS BIBLIOGRÁFICAS.....107

BIBLIOGRAFÍA.....117

INTRODUCCIÓN

Al leer la frase: "la privacidad ha muerto y las redes sociales la mataron"[1], cualquiera podría imaginar que se trata de una expresión tomada de una novela de ficción al estilo orwelliano, sin embargo, es tan sólo un extracto de la realidad actual que revela un tema de gran importancia y polémica: la protección de nuestra privacidad y de nuestros datos personales en un mundo intangible y desmaterializado de la internet y las redes sociales.

Con el advenimiento de las Tecnologías de la Información y las Comunicaciones (en adelante, TICs) el uso de la internet y las redes sociales ha crecido exponencialmente, induciendo con ello, un acelerado y alto grado de digitalización de la vida de las personas incluido el ejercicio de sus derechos y el de su identidad.

Sin embargo, esta transición ha implicado que la actividad humana, traducida en datos personales, se esparza imparablemente en el mundo inmaterial como lo es el espectro digital, y que, a su vez, adquiera un carácter cuantificable que permita su flujo y fácil acceso para que cualquiera pueda procesar estos datos, almacenarlos y transmitirlos sin límites regulatorios que tengan al alcance para garantizar su control y protección.

Lo anterior, ha ceñido un punto de inflexión crítico en materia del derecho a la protección de la privacidad y los datos personales de los ciudadanos del mundo en el ámbito digital, toda vez que la obtención de cada vez más información personal se ha constituido como la base del desarrollo de la economía global y digital actual, en el que el flujo e intercambio de datos personales es su principal insumo.

[1] Frase memorial del fundador del famoso blog, Mashable, Pete Cashmore, en, *Privacy is dead, and social media hold smoking gun*. Dirección URL: http://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/ [consulta: 27 de enero, 2020].

En los últimos años, este fenómeno se ha manifestado de manera sobresaliente en las redes sociales como importantes vertientes tecnológicas del momento. Debido a su alta popularidad e imprescindible uso, son plataformas que presentan una gran exposición de inconmensurables cantidades de datos personales concernientes a los usuarios y no usuarios, que revelan casi de manera exacta su identidad y vida diaria.

Esto ha propiciado que, a la luz de las ventajas que demuestran las redes sociales, tanto en nuestro país como el resto del mundo, dichas plataformas se configuren como una gran fuente para la extracción ilícita de datos personales, así como el principal medio para su tratamiento ilegal y vulneración de las personas y sus derechos.

En este contexto, se ha hecho apremiante la institucionalización del derecho a la protección de datos personales con el fin de garantizar no sólo la protección de este tipo de información de una persona, sino de establecer un habilitador para el ejercicio de otros derechos, los cuales no pueden ser ejercidos con libertad ante el riesgo de que la persona pueda ser afectada si se ocupa su información personal indebidamente.

Cabe señalar que, el que exista una protección a los datos personales frente a la tecnología, en este caso, las redes sociales, no significa impedir el proceso electrónico de informaciones necesarias para el funcionamiento de cualquier país en pro de la modernidad, sino buscar asegurar su uso con una perspectiva en pro del derecho a la protección de aquella información personal que se encuentra almacenada en las plataformas sociales ya que, “cuanto más influyen la tecnología y el flujo de datos en las estructuras sociales, más importancia cobran la intimidad y la protección de datos entre la población”[2] para mantener protegidos sus derechos.

[2] Pedro Grimalt, Servera, “La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y

México no es una región ajena a la revolución tecnológica que impera actualmente a nivel global, sin embargo, presenta un escenario en el que la mayoría de la población desconoce el valor de sus datos personales, así como el derecho que los protege, lo cual se ha traducido en un alto índice de afectaciones y vulnerabilidades a la población en el uso de herramientas tan imprescindibles.

En nuestro país existen múltiples áreas de oportunidad tal como el combate a la corrupción, prioridad que podría llevar a pensar que la protección de datos no resulta un tema de primera necesidad, no obstante, lo es, es un tema de primera necesidad en tanto que un tratamiento inadecuado de datos personales puede llegar a impactar en los aspectos más sensibles de la esfera de derechos de las personas.

Garantizar la protección de datos personales en el ámbito digital de las redes sociales es un tema de máxima prioridad para el Estado democrático en México. Lo anterior se debe entender no sólo desde la dimensión democrática procedimental referente a las normas de funcionamiento de las instituciones, sino desde una dimensión relativa al reconocimiento de las libertades y derechos fundamentales[3], así como de la implementación de condiciones óptimas para garantizar su afectiva expresión y en la mayor medida, el bienestar de los ciudadanos tanto en el espectro físico como digital.

A través de esta obra, se analiza, de manera general, dicha problemática en México ya que si bien, es uno de los países referentes y líderes en materia de protección de datos personales en Latinoamérica, aún tiene diversos pendientes por realizar en el aspecto de socializar y consolidar el derecho a la protección de datos personales entre su población para ser ejercido y respetado en un ámbito digital como son las redes sociales y con ello habilitar los derechos de los usuarios.

---

libertades en internet" en Julián Valero Torrijos, *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica,* p. 95

[3] Cfr. Stefano Rodotá, *Democracia y protección de datos* [en línea], p. 21. Dirección URL: https://revistasonline.inap.es/index.php?journal=CDP&page=article&op=view&path%5B%5D=690 [consulta: 27 de enero, 2020].

Por tal motivo, el objetivo del presente estudio es plantear de manera general, la importancia de garantizar el ejercicio de los derechos humanos desde el derecho a la protección de datos personales, en las redes sociales como nuevos espacios de interacción social, con el fin de mitigar los riesgos y vulneraciones digitales que afectan los derechos de la población como consecuencia de tratamientos inadecuados en estos espacios sociales.

Las ideas aquí plasmadas tienen la intención de posicionar esta problemática como parte de la práctica de la interacción social en el mundo digital así como coadyuvar a que este espacio inmaterial, sea cada vez más un espacio seguro desde una cultura de responsabilidad social en materia de protección de datos personales y fortalezca el protagonismo de los ciudadanos como dueños de la vida pública digital que conlleve a consolidar una sociedad más democrática en el uso de servicios digitales como las redes sociales.

El estudio en comento no sólo tiene un fin descriptivo respecto al reconocimiento de la protección de datos personales en el ámbito de las redes sociales y sus implicaciones que vulneran los derechos y libertades de los usuarios y no usuarios de estas herramientas tecnológicas, sino también prescriptivo, es decir, busca proponer un factor concreto y objetivo para la atención de este nuevo dilema, el factor de los usuarios.

Para ello se analiza en primer lugar, la protección de datos desde un marco teórico-conceptual y su distinción con otros conceptos como privacidad, intimidad y vida privada; así como su evolución como derecho en México.

De manera particular, se aborda lo relativo al impacto que tiene la existencia de grandes cantidades de datos personales expuestos en las redes sociales por los usuarios, así como las diferentes formas de vulneración a la protección de datos personales y las amenazas informáticas que se han configurado a partir de este espectro digital, con el fin de entender la complejidad y diversidad de los riesgos y, por ende, hallar las medidas que pudieran aplicarse para su solución.

Asimismo, se analizaron diversas investigaciones realizadas con soporte en diferentes referentes para ofrecer un panorama general de México sobe cifras relevantes relativas al uso del internet y el uso de las redes sociales, de manera que sirvan para dimensionar el alcance de dichos servicios y la penetración que ha tenido en el número de internautas mexicanos.

Finalmente, se exhibe una muestra de diferentes cifras acerca del nivel de cultura que coexiste en la población mexicana con el objetivo de analizar la relación del conocimiento y ejercicio del derecho a la protección de datos personales que permita brindar un panorama general actualmente en México.

CAPÍTULO 1. MARCO TEÓRICO DE LA PROTECCIÓN DE DATOS PERSONALES

"La mera intromisión en la privacidad del individuo se considera en sí misma un acto reprobable y atentatorio contra la dignidad y libertad de la persona."

Ana Isabel Herrán Ortiz[4]

1.1 ¿Qué son los datos personales?

Toda información concerniente a una persona física, que la identifica o la hace identificable, ya sea de manera directa o indirecta, constituye lo que se denominan datos personales. Los datos personales son una expresión de identidad, que retratan quién es una persona, sus características y comportamientos y que la identifican como individuo único distinguido del resto.

Los datos personales pueden ser de diferentes tipos, por ejemplo, datos identificativos (como nombre, número de CURP, domicilio, teléfono móvil o fijo, correo electrónico etc.); datos laborales; datos patrimoniales que pueden referir a la capacidad económica de las personas y los recursos que posee; datos sobre el nivel de educación; datos de ideología o creencia; datos de salud e incluso de mayor complejidad como los datos biométricos, relativos a las características físicas, fisiológicas o conductuales de una persona; así como los datos genéticos.

De igual forma, datos relacionados con aspectos de nuestras actividades diarias como los lugares que se frecuentan o visitan, incluso los lugares donde se compra ropa pueden ser considerados datos personales.

Si bien, esta información personal aisladamente puede resultar irrelevante, el conocimiento de estos datos y su relación en conjunto con otros, podrían revelar aspectos que identifiquen a una persona, perfilarla u ofrecer una imagen de ella y

[4] Ana Isabel Herrán Ortiz, *La violación de la intimidad en la protección de datos personales*, p. 3

de su comportamiento, aficiones, preferencias, lugar de trabajo u hogar, gustos, incluso podrían revelar cuestiones más íntimas de la persona como su estado de salud, preferencia sexual o preferencias políticas.

Este tipo de datos personales se manejan hoy en día gracias a novedosos métodos de recolección de información automática como es el Sistema de Posicionamiento Global (GPS) o la geolocalización en tiempo real. Estos mecanismos permiten que se sepa dónde está la persona, en qué momento e inclusive hasta el porqué está ahí; por ejemplo, si se detecta que una persona se encuentra cercana a un hospital, se podría deducir, con ayuda de algunos otros datos, si accede al hospital, a qué especialidad acude y hasta dar con el padecimiento.

Aunado a lo anterior, conviene señalar que, los datos personales también refieren a la información de nuestra interacción en internet. Tal como se explicó en el ejemplo anterior, si de nuestras actividades diarias y comportamientos pueden derivar gran cantidad de datos personales, lo mismo sucede cuando se "navega" por internet, principalmente en las redes sociales, ya que se pueden dar a conocer directamente datos de carácter personal como el nombre, edad, gustos, hábitos personales, estilo de vida, información escolar, pero también información que le pertenece a otras personas como familiares, pareja, amigos o de conocidos ya sea a través de fotografías, videos o publicaciones por las que se puede determinar quiénes son.

Lo mismo pasa con los datos contenidos en nuestros teléfonos móviles: la ubicación geográfica, la lista de contactos, así como mensajes o la información de aplicaciones que se descarga, son datos personales, incluso datos de nuestros ordenadores como la dirección IP (acrónimo para *Internet Protocol*) o información generada al navegar en la red (identificación de *cookies)*.

Sin importar el tipo de datos de los que se trate, existe una categorización especial denominada de "carácter sensible" que por su relevancia merecen una especial protección. Esta sensibilidad se establece en función de dos aspectos:

1) qué tanto un dato refiere a la intimidad de una persona y;

2) al daño que la utilización indebida de estos datos podría conducir a su titular a ser objeto de acciones discriminativas o llevar a éste a un grave riesgo.

Por lo que, de manera enunciativa más no limitativa, podrían determinarse como datos sensibles los que pudieran revelar aspectos relativos al origen racial o étnico; estado de salud; información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas o preferencias sexuales, características físicas, fisiológicas o conductuales de una persona, entre otros.

Si bien, los datos personales corresponden, como ya se mencionó, a la información personal de un individuo que revela todo lo relativo a quién es y lo que hace; su relevancia empieza cuando son tratados por terceros ya sea que estén sujetos de tratamiento por parte del poder público gubernamental o por el sector privado.

En este orden de ideas, un tratamiento de datos personales refiere a toda acción o acciones que se les aplican a los mismos -por cualquier medio- relacionadas con su obtención, registro, utilización, almacenamiento, comunicación, acceso, divulgación, transferencia, etc.

Existen múltiples propósitos por los que se tratan datos personales, ya sea para adquirir algún bien o servicio, físico o electrónico, tal como cuando se solicita una tarjeta de crédito o alguna suscripción por internet; para mantener relaciones laborales, comerciales o de otro tipo al brindar datos de identificación o documentos sobre la escolaridad o cuestiones financieras; para establecer medidas de seguridad y control al registrar huellas dactilares de entrada a determinado sitio o reconocer el rostro de alguien para desbloquear el celular; por mencionar algunos ejemplos.

Es innegable que no hay actividad pública o privada que funcione sin la utilización de datos personales. Sin el manejo de los datos sería imposible y complicado recibir algún servicio o relacionarse con el mundo, y mucho menos se puede imaginar el buen funcionamiento de la vida electrónica sin el constante intercambio de datos de carácter personal toda vez que estos "se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores públicos como privados"[5]

De este modo, los datos personales son un elemento de valor, en función de los intereses del titular como de las instituciones públicas y las empresas, sin embargo, su obtención y uso inadecuado y descontrolado, ya sea por el propio Estado o por entes privados, podría perjudicar gravemente a sus dueños por lo que deben ser protegidos ante todo tratamiento que les sea aplicable.

1.2 Vida Privada, privacidad e intimidad

Una vez definido qué es un dato personal, para estudiar el derecho a la protección de datos personales es preciso destacar el proceso evolutivo de este derecho humano y su distinción con otros derechos de la personalidad como lo es la vida privada, privacidad e intimidad.

La primera generación de derechos, propia de la época del siglo XVIII fue "marcada por las libertades individuales, lo que ha constituido los derechos de defensa de la persona"[6] ante la injerencia de los poderes públicos en la esfera privada de los individuos, entre los cuales se configuran derechos como el de la vida privada, intimidad, honor o imagen.

Se entiende como vida privada el derecho de todo individuo de contar con un espacio alejado del acechamiento y conocimiento externo, es decir, "una idea

[5]Aristeo García González, *La protección de datos personales. Derecho fundamental del siglo XXI. Un estudio Comparado*, p. 745. Dirección URL: http://www.revistas.unam.mx/index.php/bmd/issue/view/922 [consulta: 27 de enero, 2020].
[6] Ibid., p. 746

extensa y genérica, que cubre todo aquello que no deseamos llegue a ser parte del conocimiento general de una sociedad en particular".[7]

La vida privada es creada y definida por el Estado mediante la ley; por lo que es el mismo Estado quien tiene la obligación de salvaguardar el bienestar personal de los ciudadanos al asegurar que no habrá intromisión de la autoridad ni de la colectividad en su esfera privada, a reserva de determinadas excepciones en las que deba intervenir y limitarla por existir riesgos en los intereses colectivos, la seguridad pública y los derechos de los ciudadanos.

El espacio de la vida privada no sólo es ajeno a toda forma de control e intrusión, es "el espacio más característico de la libertad"[8], entendiéndose a esta libertad como la posibilidad de huir de la vigilancia y escrutinio público para desarrollar con libertad e independencia su individualidad e identidad.

En este sentido, la vida privada busca garantizar el libre desarrollo de la personalidad de un individuo ya que "abarca una amplia gama de elementos y de manifestaciones de la personalidad individual"[9] que permiten que una persona se conduzca sin imposiciones sobre su actuar y sin miedo a ser merecedor de cualquier daño material o físico, o de alguna forma de violencia o humillación pública.

De esta manera se puede entender por vida privada, como un espacio amplio y generalizado, dado por la ley, cuya naturaleza es la posibilidad de exclusión de la vida pública e injerencias de terceros, además de ser un espacio de libertad para el desarrollo de la personalidad individual lejos de toda perturbación externa.

---

[7]Cfr. Fernando Escalante Gonzalbo, *El derecho a la privacidad,* p. 37

[8]Ibid., p.17

[9] Jacqueline Peschard Mariscal, "El derecho fundamental a la protección de datos personales en México" en José Luis Piñar Mañas y Lina Ornelas Núñez, *La protección de Datos Personales en México*, p. 24

La vida privada está conformada por diversos derechos individuales, como lo son el derecho a la intimidad, el honor y la imagen. Cada uno refiere a diferentes ámbitos de protección dentro de la vida privada de una persona, por lo que la defensa de estos derechos constituye "el núcleo de identidad de las personas, sus patrones, perfil personal e individual, modos de vida, propósitos y proyectos, el memorial destacado de la personalidad del individuo"[10]

Estos últimos derechos de la personalidad son, con frecuencia, confundidos entre sí en virtud de que no existe una definición categórica de ninguno de estos conceptos, sin embargo, cada uno refiere a aspectos diferentes que conforman la vida privada de las personas, por lo cual, para fines prácticos y de mayor entendimiento, se distinguirán cada uno brevemente.

El derecho al honor refiere a una doble acepción; proteger "la buena reputación que puede tener alguien frente a expresiones o mensajes que la pueden desmerecer frente a la consideración ajena y su ámbito social y protección a la consideración que tiene alguien de sí misma"[11]

Con respecto a la propia imagen, puede llegar a confundirse con el derecho anterior, sin embargo, refiere más a la facultad del titular de: "disponer de la representación de su aspecto físico que permita su identificación (…)"[12]. Un ejemplo de ello en el contexto actual son los múltiples casos de personas que publican sus fotografías en espacios cibernéticos y que, en ocasiones, son usadas sin el consentimiento de estos, vulnerando así el derecho a su propia imagen.

Por lo que se refiere a la intimidad, es vista como "la parte más reservada de la vida privada"[13], es decir, es una esfera reducida que constituye "el núcleo

[10]Juan Carlos Hernández, *La protección de datos personales en Internet y el habeas data* [en línea], p. 63 Dirección URL http://www.corteidh.or.cr/tablas/r32012.pdf [consulta: 27 de enero, 2020].
[11]Pedro Grimalt Servera, *op. cit.,* p. 71
[12] Idem.
[13]Perla Gómez Gallardo, *Libertad de expresión, protección y responsabilidades*, p. 178. Dirección URL: http://biblio.flacsoandes.edu.ec/catalog/resGet.php?resId=55166 [consulta: 27 de enero, 2020]

esencial de la personalidad"[14] ya que refiere a aspectos de un individuo como rasgos y características de su cuerpo, imágenes, pensamientos y emociones, hechos pasados propios o de la vida familiar, escritos, conversaciones, etc.

También ha sido considerada como un espacio físico y espiritual "reservado al ser humano en el que puede desarrollar todas sus potencialidades como persona […]"[15]. Incluso se determina como un núcleo dentro de la vida privada "que se desea proteger con mayor empeño por considerarlo inseparable de la esencia misma de nuestra propia persona"[16] por ser el ámbito en el que el individuo ejerce plenamente su autonomía personal[17] y lleva a cabo su vida privada.

Por otro lado, a finales del siglo XIX, surge preocupación por proteger la vida privada de las personas de injerencias provenientes de nuevas invenciones tecnológicas, como la prensa. Este nuevo derecho se fue constituyéndose como de la privacidad.

El término de privacidad tiene su precedente en la expresión acuñada al juez Thomas Cooley, "*the right to be alone"* mejor conocido como *el derecho a ser dejado solo o el derecho a estar solo*, que dotaba al individuo de una inmunidad frente a las intromisiones ilegales del gobierno, así como de la curiosidad lasciva del público general[18] para disfrutar de su vida.

Basados en esta premisa, Samuel Warren y Louis Brandeis, en 1890, publicaron un artículo titulado "*Right to Privacy*" (Derecho a la Privacidad), cuyo

[14]Ana Isabel Herrán Ortiz, *op. cit.,* p. 96
[15]Pedro Grimalt Servera, *op. cit., p.* 71
[16]Ernesto Araujo Carranza, *op. cit.,* p. 37
[17]Ernesto Garzón Valdés, *Lo íntimo, lo privado y lo público*, p. 16
[18]Cfr. María Nieves Saldaña, *The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis*, p. 206 Dirección URL: http://revistas.uned.es/index.php/derechopolitico/article/download/10723/10242 [consulta: 27 de enero, 2020]

objetivo era establecer límites jurídicos a la intromisión a la vida privada de las personas, que amenazaba el desarrollo de la prensa.[19]

Dicha publicación sentó las bases del derecho a la privacidad, entendida como "la facultad que tienen los individuos para no ser interferidos o molestados, por persona o entidad alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público"[20].

La privacidad se entiende como "el derecho que todo individuo tiene a separar aspectos de su vida privada del escrutinio público"[21]; sin embargo, la privacidad "no refiere a todos los campos de la vida privada libres de interferencia, sino a los asuntos más íntimos y personales"[22] tal como la vida familiar, relaciones amorosas, etc.

Cabe traer a colación que Herrán Ortiz (1999), explica a la privacidad como la capacidad de las personas para decidir apartarse de la vida en sociedad, lo que se traduce en una libertad de decisión ante el contacto con la sociedad y la vigilancia de terceros[23].

En este sentido, se ha determinado que la protección a la privacidad se basa en una idea de la dignidad humana[24] cuyo rasgo principal es la libertad personal de escoger y decidir sobre su vida privada. La privacidad tutelada por el derecho a la vida privada es este derecho de la persona de conciencia y decisión para separar un ámbito privado de interferencias ajenas y garantizar y proteger la libertad personal como rasgo principal de la dignidad humana.

---

[19]Cfr. Carlos G. Gregorio, "Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina", en López Ayllón, *et al. Transparentar al Estado: la experiencia mexicana de acceso a la información,* p. 301 Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf [consulta: 27 de enero, 2020].
[20]Ernesto Villanueva, "Derecho a la vida privada", en Ernesto Villanueva, *Derecho de la Información. Conceptos básicos,* p. 233.
[21]Diego García Ricci, *El derecho a la privacidad*, p. 15
[22] Cfr. Fernando Escalante Gonzalbo, *op. cit.,* p. 14
[23] Cfr. Ana Isabel Herrán Ortiz, *op. cit.,* p. 95.
[24]Cfr. Fernando Escalante Gonzalbo, *op. cit.*, p. 11

La intimidad y la privacidad son vistas como aspectos que convergen para el desarrollo personal del individuo; "la intimidad referida al mundo interior, profundo y esencial del ser humano, y la privacidad referida a esos otros ámbitos de la persona que la vinculan con el exterior, en las relaciones y actividades sociales"[25]. Es decir, la privacidad refiere a una relación de pareja y la intimidad al vínculo afectivo entre los integrantes, el cual es sólo conocimiento sólo de quienes deciden los involucrados.

1.3 Derecho a la protección de datos personales

Ahora bien, no es hasta el desarrollo de la tecnología informática, en los años setenta, que se va creando una idea distinta del derecho a la vida privada y la privacidad, una evolución respecto a su ámbito de protección.

A causa de este avance tecnológico, se concedió la posibilidad de un procesamiento automático de la información, misma que incide y refiere a la vida privada de los individuos y que permitió que a través de medios ilimitados se pudiera "conocer, tratar y ceder información personal, al grado de invadir todos los ámbitos de actuación del ser humano",[26] aumentando el riesgo de abusos y agresiones a los individuos por la disponibilidad de su información para ser utilizada de manera ilícita o que pudiera resultarles dañina.

Baste como muestra lo sucedido durante la Segunda Guerra Mundial cuando el bloque nazi (con la ayuda de los primeros procesos informáticos) utilizó datos personales de índole racial y de identidad -de los censos realizados años antes en las regiones alemanas- para invadir su privacidad y ejercer control sobre ellos, al punto de desencadenar uno de los más grandes actos de discriminación racial que terminó en el mayor genocidio de la historia.

Bajo este contexto, presidido por la tecnología, surge el derecho a la protección de datos personales como un derecho humano de tercera generación,

[25] Ana Isabel Herrán Ortiz, *op. cit., p.* 96
[26] Ibid., p. 93

para dar respuesta a fenómenos tecnológicos que permiten la creciente tendencia a generar bases de datos de carácter personal y su utilización incontrolada.

En este sentido, la vida privada y la privacidad cobran una nueva acepción en virtud de que, gracias al avance tecnológico, estos derechos se traducen en datos que revelan el ámbito privado de la persona, es decir, hay una materialización del ámbito privado, en datos personales.

Por lo tanto, "la protección de datos personales tiene que ver con el resguardo de la información concerniente a la vida privada".[27], ya que los datos personales refieren a información referente a los aspectos de este derecho.

Asimismo, el derecho a la protección de datos personales es categorizado como un derecho de la personalidad, toda vez de que defiende al sujeto de intromisiones informáticas que provoquen un mal uso de su información y, por ende, condicionen el desenvolvimiento de su personalidad en la esfera privada y ante la colectividad.

Pongamos, por ejemplo, los casos en los que se instalan cámaras de videovigilancia en las empresas, las cuales son colocadas por cuestiones de seguridad en determinados espacios. El hecho de que existan cámaras grabando las actividades de los empleados, puede inhibir el delito, pero a su vez, crea una condición que no permite que los trabajadores se manifiesten libremente dentro de la esfera social-laboral al poderse sentir "espiados", ya que la posible utilización indebida de su información por terceros priva su proceder en las actividades colectivas.

De manera que, si el derecho a una vida privada busca proteger la vida familiar, sexual, ideológica, religiosa y todos aquellos aspectos que garanticen la dignidad humana y velen por el resguardo de la esfera más íntima de la persona; el derecho a la protección de datos personales otorga el derecho a las personas de proteger y controlar su información personal que refiera a su vida privada o que

[27] Ernesto Araujo Carranza, *op. cit.,* p. 118

conduzca a ella, contra un uso inadecuado o ilegal que perjudique su identidad y libertad individual y limite el libre ejercicio de sus derechos.

Así que, el derecho a la protección de datos personales no sólo da la prerrogativa a la persona de proteger su identidad y gozar de una esfera privada en la cual pueda desarrollar su vida sin injerencias ajenas, sino que, le da la facultad de mantener un control sobre ella, una libertad de elegir el uso o no de su información personal y mantener el control sobre ella, denominada *autodeterminación informativa.*

La autodeterminación informativa permite al titular dos cosas:

1. control sobre su información personal (íntima o no íntima) y decidir si puede o no ser utilizada por otros y;
2. control sobre el uso que los otros hagan de los datos personales del titular[28], es decir, el individuo puede decidir y disponer qué información puede ser tratada y decidir quién, cómo y para qué puede usarla.

Cabe señalar que, el derecho a la protección de datos personales no sólo tutela la información relativa a la esfera privada de una persona, sino también, datos personales que aisladamente podrían ser irrelevantes o que no incidan directamente en la vida íntima o privada de la persona.

Es decir, el derecho a la protección de datos personales protege la información relativa al ámbito íntimo y privado de una persona, pero también, protege información que a simple vista podría carecer de importancia pero que alcanza significación cuando —gracias a los avances tecnológicos cada vez más sofisticados— se trata en conjunto o sea relaciona con otros datos.

Este tratamiento puede llegar a revelar aspectos que sí formen parte del núcleo íntimo o privado de una persona u ofrezcan una imagen de su personalidad

[28] Pedro Grimalt Servera, *op. cit., p.*72

que podrían perjudicarla respecto a una invasión a su vida privada o que conlleve afectaciones a sus derechos.

Por ejemplo, los lugares que frecuenta o las marcas que prefiere una persona puede ser información presumiblemente de poca relevancia, sin embargo, este tipo de datos conciernen a una determinada persona y si son tratados en conjunto podrían permitir la creación de perfiles de individuos que, frente a una utilización ilícita podría poner en desventaja o en riego a la persona, inhibir sus acciones sociales, vulnerar sus derechos y atentar contra su libertad y dignidad.

Así pues, se determina que el riesgo no está en un único dato aislado, sino en el incesante almacenamiento de estos, ya que podrían ofrecer un retrato de la persona ante terceros que puedan aprovecharlo indebidamente.

La importancia que ha llegado a adquirir este tipo de información personal referente a las preferencias y gustos, actualmente se refleja en el uso comercial que se les ha dado, ya que hoy en día, los datos personales son nombrados "el nuevo oro" en virtud de que éstos permiten la comercialización de bienes y servicios porque habilitan una imagen personalizada sobre las necesidades de las personas y por ende un mayor margen de persuasión publicitario.

De tal manera, toda información concerniente a una persona merece ser protegida frente a su uso tecnológico, ya que lo verdaderamente significativo no es el dato en sí o su naturaleza, sino la susceptibilidad para afectar al individuo, perjudicando su libertad individual y social.

Bien diría la autora Sofí Charvel Orozco (2001), "la frase 'protección de datos personales' conduce a confusión, pues el dato no necesita protección alguna. Lo que necesita protegerse es la persona vinculada al dato".[29] Por lo tanto, el bien jurídico que se protege en la protección de datos personales no es en sí los datos personales, sino la persona a quien concierne este dato.

[29]Sofía Charvel Orozco, "Bienvenida", en H. Cámara de Diputados, *Protección de Datos Personales. La voz de los actores,* p. 14

Nada de lo expuesto aquí significa que se esté ante el rechazo de la utilización informática de los datos personales, sino únicamente se presenta la necesidad de un derecho que permita controlar y vigilar este tratamiento a fin de que sea racional y no excesivo conforme a los fines para los que se recaba y así garantizar la protección del titular de los datos.

1.4 Derecho de datos personales como habilitador de otros derechos y libertades.

El derecho a la protección de datos personales no sólo ampara la necesidad de salvaguardar a la persona de injerencias externas bajo la defensa del derecho a la vida privada, sino que concede al individuo una capacidad de actuación positiva que le permite proteger sus datos personales y a su vez, sus derechos y su libertad individual, esto es, "concede al individuo, ámbitos de actuación positivos que le permitan garantizar el respeto de sus derechos"[30] y el desenvolvimiento libre de su personalidad y relaciones en los ámbitos privado y público.

De esta manera, el derecho de protección de datos personales es un derecho que se expresa como un condicionante para la tutela efectiva de otros derechos y libertades fundamentales de una persona, empezando por la vida privada y sus derechos individuales tales como el de la intimidad, el honor, la imagen o la privacidad, así como su derecho a la libertad de expresión, de acceso a la información, de participación, derecho de libre asociación, inclusive la libertad sexual.

En definitiva, el derecho a la protección de datos de carácter personal otorga a las personas el control sobre sus informaciones e impide su tratamiento para fines diversos no consentidos, al dar "reconocimiento y establecimiento de prerrogativas, principios y procedimientos para el tratamiento por parte del Estado o de terceros, de la información concerniente a personas físicas".[31]

[30] Cfr. Ana Isabel Herrán Ortiz, *op. cit.,* p. 94
[31] Ernesto Araujo Carranza, *op. cit.*, p. 33

Además, brinda al individuo la prerrogativa para defender su libertad individual, conciencia y el ejercicio de sus derechos -que conforman su identidad personal- así como su desarrollo social cuando no se reproduzca dentro de un adecuado marco de garantías.

Estas dos acepciones del derecho de protección de datos personales se encuentran intrínsecamente relacionados al desarrollo democrático. Tanto la habilitación de otros derechos fundamentales como el otorgamiento para la defensión de la libertad individual se encuentran estrechamente conectados a una cada vez más amplia dimensión de la democracia expresada en el reconocimiento de las libertades y derechos fundamentales y su efectiva realización a través de la implementación de garantías que así lo permitan.

Lo anterior toda vez que, la protección que brinda el derecho a la protección de datos personales "representa una condición preventiva para poder gozar enteramente de otros derechos fundamentales, que constituyen exactamente el núcleo de las libertades democráticas"[32] Asimismo, existe una "conexión silenciosa entre el ámbito personalísimo de la intimidad y de la privacidad, y una esfera pública democrática construida sobre libertades fundamentales"[33]

En este sentido, la democracia se encuentra construida sobre libertades fundamentales que permitan tanto el respeto y la protección de los derechos humanos en general, así como aquellos que otorguen la construcción de una ciudadanía capaz de opinar o manifestarse libremente y sin temor a represalias.

Por lo tanto, si garantizar el derecho de la protección de datos personales permite conceder al individuo una capacidad de actuación positiva para defender su libertad, la cual "se proyecta a partir del reconocimiento de los derechos inherentes a la persona que permitan su desenvolvimiento tanto en el ámbito de lo

[32] Stefano Rodotá*, op. cit.* p. 20
[33] Ernesto Garzón Valdés, *op. cit.* p. 8

público como en el ámbito de lo privado"[34] entonces también permite este valor intrínseco de la democracia, respecto a la libertad de los individuos para ejercer sus derechos y potenciar su participación.

1.4 El derecho de protección de datos personales en México

En los últimos años, México ha tenido un importante y destacado desarrollo en el marco normativo en materia de protección de datos personales, con una gran influencia europea al ser la región en la que se han sentado las bases de este derecho.

El primer precedente normativo de este derecho en México data del año 2002 con la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental que impone a las entidades públicas la obligación de proteger los datos personales que tengan a su disposición. Esta ley prevé la protección de datos personales como una limitante al derecho al acceso a la información.

Posteriormente, en 2007, la reforma al artículo 6º constitucional hace una breve referencia a la protección de la vida privada y los datos personales de los mexicanos, elevando su importancia en un rango constitucional, pero como una limitante del derecho a la información y sin un desarrollo particular y propio: "toda 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".[35]

Años después, en 2009, se reformaría el artículo 16 constitucional que incorporó de manera independiente, el derecho a la protección de la vida privada de los ciudadanos, el cual dice a la letra lo siguiente:

---

[34] María Solange Maqueo Ramírez, Alessandra Barzizza Vignau, *Democracia, privacidad y protección de datos personales*, p. 19

[35] DECRETO por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 20 de junio de 2007.

Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.[36]

De igual forma, se adicionó un segundo párrafo, en el que se reconoció plenamente la protección de datos personales como un derecho fundamental autónomo, elevándolo a un rango constitucional y separándolo del derecho a la vida privada.

Otro de los elementos importantes de esta reforma es que estipula los derechos relativos al acceso, rectificación cancelación y oposición de la protección de datos, y, además, los supuestos de excepción a los principios que rigen el derecho. Este segundo párrafo dice a la letra lo siguiente:

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.[37]

Como parte complementaria a dicha reforma, el artículo 73 también fue modificado este mismo año, estableciendo la posibilidad de que el Congreso legislara en la materia, lo que causó que en el Plan Nacional de Desarrollo 2007-2012 se estableciera la prioridad de contar con una ley federal en materia de protección de datos en la que se dispusieran los principios y obligaciones que los tratados internacionales dictan en torno a este derecho.

Cabe señalar que el reconocimiento del derecho a la protección de datos personales en la Constitución implicó que el Estado adquiriera nuevas

[36] DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 01 de junio de 2009.

[37] DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, 01 de junio de 2009.

obligaciones que pudieran ser interpretadas y exigidas a partir de parámetros desarrollados en el ámbito internacional.

En 2010, se publicó la primera ley que regula exclusivamente la protección de datos personales en posesión de instituciones privadas, la Ley Federal de Protección de Datos Personales en Posesión de Particulares. Finalmente, en 2017 se emitió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que dicta las disposiciones expresas para el tratamiento de datos personales en el sector público.

Hoy en día, el derecho a la protección de datos personales en nuestro país está regulado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y las leyes estatales de protección de datos personales, una por cada entidad, conforme a un proceso de armonización con la nueva ley general del sector público.

Asimismo, México cuenta con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) que es el organismo autónomo garante del derecho a la protección de datos personales a nivel federal. Con la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el 12 de junio de 2003, surge como el entonces, Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) para que, posteriormente en 2015, obtuviera su autonomía, convirtiéndose en lo que ahora es el INAI.

Por lo tanto, el marco normativo mexicano en materia del protección de datos personales terminó por armonizarse al contar con dos legislaciones exclusivas en el tema, en las que se plasman disposiciones para la efectiva tutela de este derecho a partir de una serie de principios aplicables a todo el ciclo de vida del tratamiento de los datos; una serie de derechos que permiten que cada individuo disponga de su información y decida sobre su utilización; las

obligaciones que garantizarán la protección y seguridad de la información que obran en posesión de los responsables, entre otras disposiciones.

Ahora bien, cuando se está ante un tratamiento de datos se contemplan tres momentos: recolección, uso y supresión, los cuales pueden llevarse a cabo a través de diversos procedimientos utilizados por el responsable, sean manuales como electrónicos, ya sea de forma escrita, de forma verbal, vía online o de manera indirecta como la captación de imágenes o video a través de video vigilancia en determinados sitios a los que se acude.

Asimismo, en cada uno de dichos momentos la legislación mexicana contempla el cumplimiento de ocho principios rectores del derecho a la protección de datos personales que representan las directrices para asegurar la garantía de este derecho, siendo "uno de los vértices sobre los que gira un sistema de protección de datos personales, puesto que los mismos se traducen en obligaciones para el responsable que trata los datos"[38]

Estos principios básicos son la licitud, lealtad, información, consentimiento, finalidad, proporcionalidad, calidad, y responsabilidad.

Licitud

En lo que refiere al principio de licitud, el responsable deberá tratar los datos personales de los que disponga sujetándose a las atribuciones o facultades que la normatividad aplicable le confiera. Sin embargo, el hecho de que se autorice a que otros tengan acceso a una información personal de manera lícita no significa que se otorgue un permiso ilimitado para hacer cualquier cosa con esa información.

[38]José Luis Piñar Mañas, y Lina Ornelas Nuñez, "Los principios de la protección de datos personales" en José Luis Piñar Mañas y Lina Ornelas Nuñez, *La protección de Datos Personales en México,* p. 58

Lealtad

La lealtad, alude al respeto sobre la confianza que el titular depositó en el responsable para proporcionarle sus datos personales y se materializará en el sentido de que su información sea tratada conforme se acordó. También concibe la obligación de no obtener a través de medios engañosos y fraudulentos los datos.

Información y consentimiento

Los principios de información y consentimiento tienen especial significación durante la primera etapa del tratamiento que consiste en la obtención de los datos por parte de los responsables ya que son elementos fundamentales que legitiman el origen de un tratamiento de datos y son punto clave a lo largo de todo el procesamiento.

El principio de información hace referencia a que, el responsable deberá informar a los titulares, a través del documento denominado aviso de privacidad, la existencia y las características principales del tratamiento al que serán sometidos sus datos personales, como quién utilizará esa información, para qué fines, con quién se compartirá y cómo se podrá ejercer los derechos al respecto.

El aviso de privacidad deberá ser dado a conocer antes de que se proporcione la información personal y se inicie cualquier tipo de tratamiento; deberá ser sencillo, escrito en lenguaje claro y comprensivo, de fácil entendimiento y con información necesaria.

El consentimiento es un principio derivado de la obligación del responsable de informar, ya que, una vez dado a conocer el aviso de privacidad, previo al tratamiento de los datos personales, el responsable deberá obtener el consentimiento del titular el cual siempre deberá ser informado, libre, inequívoco y específico.

El consentimiento es "una declaración de voluntad procedente del sujeto titular de los datos personales por la que ésta acepta que los mismos sean sometidos a tratamiento"[39] y es la principal forma de legitimar el tratamiento en virtud de que el derecho a la protección de datos consiste justo en la facultad del individuo de tener el control y poder de decisión sobre su información personal manifestándose en este principio.

Por ende, si la persona a la que le pertenecen los datos no es capaz de tener la información precisa sobre el tratamiento de su información personal, no podrá brindar su consentimiento y, por ende, el tratamiento no será legal ni leal.

Finalidad

Por lo que respecta al principio de finalidad, los responsables únicamente podrán utilizar los datos personales para los propósitos que fueron informados en el aviso de privacidad y si fuera el caso de querer ocuparlos con intenciones diversas no establecidas en este documento, se deberá recabar el consentimiento aparte para este fin.

Proporcionalidad

La proporcionalidad apunta a que los datos personales para su tratamiento sean adecuados, relevantes y estrictamente necesarios, es decir, que sean apropiados, indispensables y no excesivos para el cumplimiento de las finalidades que motivaron su obtención y se deberá solicitar el menor número posible de datos personales.

Un ejemplo de ello es lo que sucede con los permisos de las aplicaciones móviles que solicitan infinidad de permisos de acceso a funciones del dispositivo

[39]María Belén Andreu Martínez, y María Carmen Plana Arnaldos,, "El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico", en Julián Valero Torrijos, *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica* p. 133

en el que se pretendan descargar. Estos permisos, en su gran mayoría son injustificables para el funcionamiento del programa que se va a operar, por ejemplo, que se trate de una app de juegos que solicite acceso a los mensajes enviados, fotografías, ubicación o a información de otras aplicaciones.

Calidad

El principio de calidad hace referencia a que los datos personales manejados serán exactos y correctos, completos y actualizados para los fines para los cuales se obtuvieron.

De igual forma, y con especial énfasis, los datos personales sensibles deben tener especial cuidado en su tratamiento ya que sólo si es realmente necesario entablar un tratamiento de ellos, será ineludible el estricto apego de cada principio durante su tratamiento.

Responsabilidad

Finalmente, el principio de responsabilidad, que contempla el deber del responsable de adoptar políticas e implementar mecanismos para asegurar y acreditar el cumplimiento de los principios, deberes y demás obligaciones establecidas en la normatividad aplicable; así como establecer aquellos mecanismos necesarios para evidenciar dicho cumplimiento ante los titulares y las instituciones rectoras del derecho.

Aunado a los principios ya mencionados, cabe señalar que los responsables están obligados a resguardar la seguridad de los datos personales que les fueron proporcionados bajo medidas adecuadas que eviten su pérdida, alteración, acceso o tratamiento no autorizado.

También, deberán tratar con confidencialidad los datos que obren en su posesión, evitando su difusión o comunicación con terceros sin que exista consentimiento previo para ello o algún mandato legal que lo determine.

Indiscutiblemente, estos principios son los ejes rectores del derecho a la protección de datos personales, y "constituyen su núcleo básico o esencial y por lo tanto cualquier fallo o violación de los mismos implica una violación del propio derecho"[40], sin embargo la legislación también tiene previstos una serie de derechos para que las personas puedan ejercer de forma efectiva el control de su información personal ya que "los principios para ser efectivos requieren el reconocimiento, la garantía, y tutela de los derechos de acceso, rectificación, cancelación y oposición"[41] a los cuales se les conoce como derechos **ARCO**, acrónimo conformado por las iniciales de cada uno.

A El derecho de acceso permite a la persona acceder a la información que sobre ella tiene un responsable, de dónde la obtenido, y a quién se la ha transferido, de igual forma, permite conocer las finalidades del tratamiento de los datos.

R El derecho a la rectificación permite la corrección de la información sobre aquellos datos que resulten ser incompletos, inexactos o estén desactualizados y deberá ser acompañada de la documentación que justifiquen la procedencia de lo solicitado.

C Por otra parte, el derecho a la cancelación permite la supresión o el cese de los datos en el tratamiento por parte del responsable ya sea porque ya no existe relación con el mismo o porque los datos son inadecuados o excesivos a partir de un bloqueo para proceder posteriormente a la supresión.

Este derecho responde a un tratamiento que no esté siendo apegado a los principios y deberes que marca la ley, por lo que cualquier persona, una vez percatada de lo anterior podrá solicitar, mediante documentación que lo compruebe, la voluntad de interrumpir el tratamiento.

O Por último, está el derecho de oposición permite que el titular manifieste el impedimento a que se lleve a cabo el tratamiento de sus datos personales o exigir

[40]José Luis Piñar Mañas, y Lina Ornelas Nuñez, *op. cit.,* p. 43
[41]Ibid, p. 53

su cese cuando exista una causa legítima que cause perjuicio a la persona, o para oponerse a fines específicos como cuando se usan los datos para actividades de publicidad y prospectiva comercial, sin embargo, no procederá este derecho siempre que el tratamiento sea necesario para el cumplimiento de una obligación legal.

Hay que mencionar que el ejercicio de estos derechos a la par que los principios, tienen sus límites, ya que ningún derecho es absoluto, por lo que, cuestiones como la seguridad nacional; salud pública o la afectación a otros derechos de terceros, serían excepciones para negar estas disposiciones.

1.5 Marco jurídico internacional del derecho a la protección de datos personales

Como se ha mencionado, el derecho a la protección de datos personales y la normativa que lo protege y garantiza, responde a retos del crecimiento de las sociedades modernas frente a la protección de los riesgos que contraen las nuevas tecnologías y su gran capacidad para que los gobiernos pudieran utilizar las informaciones de los individuos, invadir su vida privada y tener control sobre ellos.

Así pues, entre los años 1960 y 1970, se inició una fuerte demanda de normas específicas para regular la recolección y manejo de información personal. En un inicio se tutelaba de forma indirecta por medio de disposiciones internacionales referentes a la protección del derecho a la vida privada toda vez que "la protección de lo privado es una de las condiciones básicas de la estructura social moderna y uno de los rasgos indispensables de un orden jurídico legítimo".[42] Sin embargo, poco a poco el derecho a la protección de datos personales se iría desprendiendo de este derecho para constituirse como un derecho autónomo e independiente.

[42]Escalante Gonzalbo Fernando, *op. cit.,* p. 21

De este modo, existen diversos instrumentos internacionales que constituyen los precedentes que fundamentan el derecho a la protección de datos personales, entre los que se destacan los que a continuación se desarrollan.

En 1948 la Asamblea General de las Naciones Unidas en París, proclama la Declaración Universal de Derechos Humanos (DUDH), que establece por primera vez un marco de derechos humanos fundamentales inherentes a cualquier persona y constituyen la base para una sociedad democrática.

Este instrumento es de relevancia internacional ya que es el primero en el que se prevé, en su artículo 12, el derecho de los individuos a no ser objeto de injerencias arbitrarias a su vida privada que, si bien, no determina específicamente la protección a datos personales, incluye la intromisión a la vida privada considerada como precedente y ámbito del que forma parte el derecho que concierne a esta investigación.

Posteriormente, en 1950, el Consejo de Europa adopta el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), mejor conocido como la Convención Europea de Derechos Humanos que establece la protección a los derechos humanos y libertades fundamentales de los ciudadanos de los estados miembros.

Inspirados en la DUDH, el CEDH establece en su artículo 8[43] el derecho al respeto a la vida privada y familiar, de su domicilio y de su correspondencia ante injerencias de la autoridad.

A finales de los años sesenta, con la Recomendación 509 sobre Derechos Humanos y Desarrollos Científicos y Tecnológicos Modernos emitida en 1968 por el Consejo de Europa, se abordó la preocupación generada por las posibles afectaciones a los derechos de privacidad y vida privada de las personas derivado del acelerado progreso en los avances tecnológicos, como fueron la intervención

[43]Convenio Europeo de Derechos Humanos, [en línea]. Dirección URL: https://www.echr.coe.int/Documents/Convention_SPA.pdf [consulta: 27 de enero, 2020].

telefónica, el espionaje, el análisis estadístico para obtener información y la publicidad subliminal.

Este instrumento reconoció las libertades fundamentales y derechos humanos de todas las personas y con ello el derecho a la privacidad, ante la falta de normatividad para combatir estas amenazas a la privacidad.

Un año después, en 1969, se adopta la Convención Americana de Derechos Humanos[44], conocida como el Pacto de San José de Costa Rica que en su artículo 11 hace referencia a la protección de la honra y el reconocimiento de su dignidad sin ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

A la par que los demás instrumentos, tampoco adopta el concepto del derecho a la protección de los datos personales en sentido estricto, sólo hace referencia a conceptos vinculados a la protección de la información personal.

Definitivamente para la época en la que se redactaron estos instrumentos normativos internacionales, los avances tecnológicos no representaban el mismo grado de riesgo del manejo de información personal que implica hoy en día, sin embargo, constituyen las primeras aproximaciones jurídicas al derecho a la protección de datos personales, y devienen del reconocimiento del derecho fundamental a la vida privada y familiar, como lo demuestran cada uno de ellos.

Es en los años ochenta cuando la Organización para la Cooperación y el Desarrollo Económicos (OCDE) emite el primer documento que establece como tal el derecho a la protección de datos personales, las *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, mejor conocidas como Directrices de Privacidad de la OCDE, las cuales tuvieron como

[44]Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (b-32) San José. Dirección URL: https://www.oas.org/dil/esp/tratados_B32_Convencion_Americana_sobre_Derechos_Humanos.pdf [consulta: 27 de enero, 2020].

objeto unificar las pautas de referencia internacional para los estados miembros en materia de protección de la privacidad y los datos personales ya que la inexistencia de esta uniformidad, dificultaba el flujo de los datos personales entre los mismos estados.

Sin embargo, es hasta 1981, que el Consejo Europeo adoptaría el Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal que establece los principios y derechos que cualquier legislación debe recoger para proteger los datos personales. Asimismo, se instaura como el primer tratado internacional vinculante para los estados suscritos al mismo.

Este documento es de gran importancia ya que reconoce como tal el derecho a la protección de datos como base para fortalecer el derecho a la vida privada, además de que no sólo prevé el derecho a la protección de estas informaciones, sino, su libre circulación.

Es decir, el Convenio 108 es un estándar internacional, que une dos enfoques, el sentido de protección a los derechos humanos y la perspectiva económica que refiere al libre flujo de datos personales entre estados ya que establece las pautas para las transferencias entre los países suscritos al mismo, que cuenten con medidas de igual o mayor nivel de protección que estos para permitir el intercambio de datos con la venia de una protección similar o mayor.

En 2001, se estableció el Protocolo adicional del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos.

La Organización de las Naciones Unidas emitió en 1990 la Resolución 45/95 por la que se establecen las Directrices para la regulación de los archivos de datos personales informatizados que incluyeron los principios mínimos que deben contemplar las legislaciones nacionales en materia de protección de datos personales.

En el marco de una economía cada vez más globalizada y transfronteriza en la década de los 90, la Unión Europea buscó integrar la libre circulación de los datos personales dado su valor económico en las transacciones comerciales en la constitución de un mercado interior, por lo que adoptó en 1995 Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de personas físicas en los que respecta al tratamiento de datos personales y la libre circulación de estos datos, y la cual fue una gran influencia para las legislaciones de América Latina.

En 2000, la Carta de los Derechos Fundamentales de la Unión Europea, reconoce por primera vez a la protección de datos de carácter personal como un derecho autónomo e independiente del derecho a la vida privada y la intimidad ya que prevé un artículo específico para este derecho.[45]

De manera más reciente, en 2003, surge la Red Iberoamericana de Protección de Datos (RIPD) en La Antigua, Guatemala, con motivo de los acuerdos alcanzados en el Encuentro Iberoamericano de Protección de Datos en el que participaron 14 Estados de la región con el fin de producir iniciativas y proyectos relacionados con el derecho de protección de datos en Iberoamérica y fomentar el intercambios de experiencias e información entre ellos y así establecer instrumentos jurídicos que garanticen el derecho a la protección de datos.

Ha sido tal la importancia de este foro que, en 2017, se adoptaron los Estándares de Protección de Datos para los Estados Iberoamericanos que sirven como estatutos referenciales para las regulaciones ya existentes o las que los estados parte, establezcan en el futuro.

Por otro lado, en 2009, derivado de la 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada en Madrid, se adoptó la Resolución de Madrid sobre Estándares Internacionales sobre Protección de

[45] En su artículo 8 establece que: "Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan" mientras que en el artículo 7, disponen lo relativo a la protección de la vida privada y familiar, haciendo una clara separación entre ambos derechos.

Datos Personales y Privacidad cuya finalidad es la definición de conjuntos de principios y derechos para la efectiva protección de la privacidad en relación al tratamiento de datos de carácter personal, además de facilitar el flujo transfronterizo de los datos personales.

Finalmente, en 2016, entra en vigor el nuevo Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés), de la Unión Europea, 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 sustituye a la antigua Directiva de 1995.

Este nuevo reglamento es hasta hoy, la norma más estricta en materia de protección de datos, siendo obligatoria para todas las empresas que traten datos de cualquier ciudadano de la Unión Europea, independientemente del lugar de residencia de la empresa. Además, establece un conjunto de disposiciones de gran actualidad y vanguardia al ser diseñadas conforme a los retos que la realidad tecnológica actual demanda en cuanto al flujo de datos personales que implica el avance del Internet.

Tabla 1.1
***Instrumentos Internacionales de protección de datos personales*.**

Organismo Internacional	Instrumento jurídico	Año de emisión	Actualizaciones
Asamblea General de las Naciones Unidas	Declaración Universal de Derechos Humanos (DUDH)	1948	No aplica
Consejo de Europa	Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH)	1950	No aplica
Consejo de Europa	Recomendación 509 sobre Derechos Humanos y Desarrollos Científicos y	1968	No aplica

	Tecnológicos Modernos		
Organización de los Estados Americanos (OEA)	Convención Americana de Derechos Humanos o Pacto de San José de Costa Rica	1969	No aplica
Organización para la Cooperación y el Desarrollo Económicos (OCDE)	Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales	1980	En 2013 se actualizan las directrices.
Consejo Europeo	Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal	1981	En 2001 se establece Protocolo adicional del Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos. Actualmente se trabaja en el Convenio 108 plus relativa al internet y las nuevas tecnologías
Organización de las Naciones Unidas (ONU)	Resolución 45/95 por la que se establecen las Directrices para la regulación de los archivos de datos personales informatizados	1990	No aplica
Consejo Europeo	Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de personas físicas en los que respecta al tratamiento de datos personales y la libre circulación de estos datos	1995	2016 se sustituye por el Reglamento General de Protección de Datos 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

Consejo Europeo	Carta de los Derechos Fundamentales de la Unión Europea	2000	No aplica
31º Conferencia Internacional de Autoridades de Protección de Datos y Privacidad	Resolución de Madrid. Estándares Internacionales sobre Protección de Datos Personales y Privacidad	2009	No aplica
Red Iberoamericana de Protección de Datos (RIPD)	Estándares de Protección de Datos para los Estados Iberoamericanos	2017	No aplica

Fuente: Elaboración propia

Los instrumentos normativos internacionales antes referidos sientan las bases para el reconocimiento y difusión del derecho a la protección de datos en las legislaciones de países del mundo, desde la ley pionera en la materia, la Ley de Protección de Datos del Estado alemán de Hesse; como la *Privacy Act* de Estados Unidos (1974) que establece las bases de los principios esenciales configuradores del núcleo esencial del derecho a la privacidad; la Ley Francesa relativa a la Informática, los Ficheros y las Libertades (1978) o la Ley sobre la utilización de datos en tratamientos informáticos de Luxemburgo (1979) y así cada nación.

Es necesario recalcar que el modelo europeo ha sido un referente jurídico en materia de protección de datos personales que se ha esparcido en el resto de los países del mundo. Este derecho aparece en Europa como herencia de las experiencias ocurridas en la Segunda Guerra Mundial, por la "experiencia histórica de persecución asistida por la disponibilidad de datos personales, percepción que produce una conciencia pública a favor de la protección de datos"[46].

De esta manera, el modelo europeo ha considerado estricta y prioritaria la protección de datos personales ante los efectos nocivos que su empleo ilícito informático trae consigo, contemplado su valor económico debido al enfoque

[46] Carlos G. Gregorio, *op. cit.,* p. 312

económico globalizado y transfronterizo en el que las transacciones comerciales demandan la libre circulación de datos personales.

Por su parte, y sin entrar a profundidad en el análisis de la situación en esta región, el modelo de Estados Unidos está configurado sectorialmente, de manera que la protección de datos es abordada desde ámbitos muy específicos y generalmente locales, como la protección de la información de salud, el cuidado de los datos de los consumidores y sus transferencias sin consentimiento para fines comerciales o la protección de datos de menores.

Dicho modelo más que tener un marco federal o general como sucede con la Unión Europea apuesta por políticas autorregulatorias para las empresas, y marcos regulatorios catalizados a determinados sectores o industrias

Finalmente, en lo que respecta al caso latinoamericano, "la protección de datos fue vista como una necesidad resultado de la explosión tecnológica"[47], las recientes reformas constitucionales en algunos países han introducido este derecho y se ha generado regulación en la materia con cierta semejanza con la legislación europea y las leyes sectoriales estadounidenses, más no se ha presentado un desarrollo homogéneo en la región.

1.6 Protección de datos personales y la evolución tecnológica

Llegados a este punto, es importante prestar atención a la manera en la que se producen, almacenan y circulan los datos personales en la actualidad.

Si bien, la protección de datos personales no es nueva, son cada vez más las actividades que el ser humano realiza a través de nuevos fenómenos tecnológicos como las TIC, el Internet, las redes sociales, el Big Data, las aplicaciones móviles, el Internet de las Cosas, etc., los cuales plantean nuevas cuestiones para la protección de datos personales de los usuarios como para otros

[47] Ibid, p. 310

derechos, ya que suponen una novedosa manera de recabar grandes cantidades de datos de carácter personal.

La identificación de personas a través de cámaras de video vigilancia, las medidas de autenticación por medio de reconocimiento facial, iris, voz o huella dactilar; la utilización de motores de búsqueda; la toma de decisiones por algoritmos basados en inteligencia artificial; el envío masivo de publicidad dirigida; así como las interacciones impersonales vía redes sociales, son situaciones en las es cada vez mayor la intromisión a la vida privada ya que la posibilidad de captar, almacenar o trasmitir información personal se hace de forma ilimitada.

Por lo tanto, la necesidad de proteger en este tipo de medios electrónicos los derechos individuales, en específico el derecho a la protección de datos personales se ha vuelto inminente; principalmente en los medios de mayor incursión en la sociedad por su popularidad y novedad como lo son, actualmente, las redes sociales que por su naturaleza pueden implicar múltiples amenazas a la privacidad y protección de datos personales de una persona.

El objetivo del derecho de protección de datos, consistente en evitar la recolección y procesamiento ilegal de los datos personales por parte de terceros, ha trasladado su ámbito de protección de una dimensión física a un nuevo espacio público digital. En ambos espectros resulta indispensable garantizar la libertad y dignidad humana de una persona protegiendo sus datos personales.

A continuación, se abordará a profundidad aspectos generales sobre el internet y el uso de las redes sociales; cómo se han desarrollado a lo largo del tiempo y las implicaciones que tienen en el tema de la protección de datos personales en esta nueva realidad digital.

CAPÍTULO 2. EL NUEVO ESPACIO PÚBLICO DIGITAL: INTERNET Y LAS REDES SOCIALES

"Si aceptamos como algo normal que todo en nuestra vida puede ser agregado, vendido o filtrado en caso de un hackeo, entonces estamos perdiendo mucho más que nuestros datos personales, perdemos la libertad de ser humanos"

Tim Cook[48]

Hoy en día, escuchar o hablar sobre internet y más aún sobre las redes sociales, resulta un tema bastante común. Los beneficios que han traído consigo las han convertido en objeto de elogios y popularidad al permitir que las personas se relacionen de una manera rápida, sencilla y accesible con el resto del mundo, a través de la interconectividad y el uso e intercambio de grandes cantidades de información como nunca se había visto.

Sin embargo, estas herramientas tecnológicas también poseen implicaciones negativas en su funcionamiento. Lo anterior debido a que se han producido significativos cambios en los modos de apropiación social de este tipo de medios de comunicación digitales de masas, potencializando la manifestación de expresiones de violencia hacia los usuarios, coartando su libertad dentro del espacio digital y sus derechos, principiando por su privacidad y sus datos personales.

2.1 Internet

Como bien se dijo, los años setenta fue la época de los inicios de la informática, cuya expresión se forma de la unión de las palabras *información* y *automática*, haciendo alusión a los tratamientos automatizados de la información, incluida los datos personales. A partir de este nuevo fenómeno tecnológico, aparecen los primeros dispositivos informáticos, como las computadoras para la industria empresarial y gubernamental, seguidas de ordenadores domésticos de escritorio y

[48]Cita del discurso del CEO de Apple, en Eduardo Arcos, "El inspirador discurso de Tim Cook en la Universidad de Stanford: «Sean diferentes, dejen al mundo creaciones que tengan valor". Dirección URL: https://hipertextual.com/2019/06/inspirador-discurso-tim-cook-universidad-stanford-sean-diferentes-dejen-mundo-creaciones-que-tengan-valor [consulta: 27 de enero, 2020].

los posteriores ordenadores portátiles de uso individual, hasta los más novedosos aparatos como la tableta electrónica o celular inteligente también conocido como *Smartphone*.

El desarrollo informático significó el inicio de una nueva era que trajo consigo nuevas manifestaciones tecnológicas vinculadas a novedosos servicios de información y comunicación de gran trascendencia que se denominaron Tecnologías de la Información y Comunicación, (TIC).

De acuerdo con la OEA, las TIC son tecnologías que permiten un intercambio de cualquier tipo de información de manera remota, que puede ser vista o leída por terceros receptores de un modo similar a quienes la emitieron. De igual forma, permiten un procesamiento y almacenamiento de datos e información de gran escala e incluso una automatización de las actividades realizadas.[49]

Como ejemplos del conjunto de tecnologías que forman parte de las TIC se encuentran la telefonía móvil, la televisión digital, formatos de contenido audiovisual, la internet, entre otras, las cuales facilitan la difusión de información y comunicación entre personas a grandes distancias a través de la "convergencia tecnológica de la electrónica, el software y las infraestructuras de telecomunicaciones."[50]

La expansión de las TIC y especialmente de la internet se convirtieron en fenómenos tecnológicos de gran relevancia para la sociedad y la economía del siglo XX, sin embargo, fue en el siglo XXI en el que se dio su carácter determinante en estos ámbitos, dando lugar a una nueva etapa de la sociedad en

[49]Organización de los Estados Americanos (OEA), "Sobre e-Gobierno" [en línea]. Dirección URL:http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx [consulta: 27 de enero, 2020].
[50]César D. Vargas, *La globalización del e-gobierno y la transparencia de la información pública*, p. 69

torno a esta base tecnológica, conceptualizada como “Sociedad de la Información”[51].

Internet es la tecnología más sobresaliente referida a las TIC por ser el medio que ha crecido a mayor velocidad y que más se ha popularizado a lo largo de la historia. Es el fenómeno tecnológico más grande de todos los tiempos debido a las ilimitadas posibilidades que ofrece para acceder a todo tipo de información y formas de comunicación, así como a incalculables bienes y servicios de forma sencilla e inmediata.

Internet es definida como una red de redes en la que se comparten y comunican datos y recursos a través de una interconexión a nivel mundial entre ordenadores y los propios usuarios[52] y a la que grandes corporaciones, gobiernos, instituciones, y usuarios comunes tienen acceso, haciendo menores las distancias[53].

El primer indicio del origen de esta red data de finales de los años sesenta, en campos universitarios estadounidenses con su antepasado *Arpanet*[54] posteriormente la internet nace en 1983 cuando diversas redes informáticas con la misma tecnología se unen creando la llamada red de redes[55] cuya expansión a partir de ese momento, ha sido imparable.

Durante los años noventa, internet pasó de ser una simple conexión entre universidades y se planteó como una plataforma para generar conocimiento e información gracias a la invención del navegador denominado *Word Wide Web* mejor conocido con las siglas “www”. Con ello, internet se volvería la tecnología

---

[51]Cfr. Fundación Kaleidos**,** *Proximidad en el ámbito local. Proximidad, nuevas tecnologías y participación ciudadana en el ámbito local*, p. 21

[52]A. Luengo López, *Adicción a Internet: conceptualización y propuesta de intervención* [en línea], p. 22. Dirección URL: http://www.jogoremoto.pt/docs/extra/BL5L6u.pdf [consulta: 27 de enero, 2020].

[53]Víctor Drummond, *Internet, Privacidad y Datos Personales,* p. 25

[54] Manuel Castells, “Internet, libertad y sociedad; una perspectiva analítica”, p. 6. Dirección URL: http://journals.openedition.org/polis/7145 [consulta: 27 de enero, 2020].

[55]Ana Garriga Domínguez, *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*, p.20.

con mayor expansión de todos los tiempos, debido a sus millones de usuarios de todo el mundo, convirtiéndose en una herramienta de alcance mundial

De conformidad con la Unión Internacional de Telecomunicaciones de la ONU, se estima que, a finales de 2019, poco más de la mitad de la población mundial es usuario de internet, es decir, 4.1 mil millones de personas en todo el mundo[56]

Ante tal expansión, internet se ha concebido como un espacio que propicia el ejercicio de derechos y libertades ciudadanos como la libertad de expresión y el acceso a la información, los cuales garantizan un nuevo ámbito para la opinión pública libre y con ello el pluralismo de una sociedad democrática. Es un "espacio público de debate, de relación, de proposición, y, por tanto, parte cada vez más importante del proceso democrático en su conjunto"[57]

Por ejemplo, la libertad de expresión se ejerce mediante la publicación de tuits, blogs, comentarios en videos o páginas debate incluso el seleccionar un "me gusta" en cualquier red social. Derechos de participación política y de acceso a la información y transparencia gubernamental se practican a través de la información pública que es compartida en páginas oficiales gubernamentales en redes sociales, ya sea videos de sesiones públicas o avisos sobre acciones públicas.

El derecho de libre asociación se ha trasladado al ámbito también de las redes sociales, a través de foros, grupos o mensajes privados, los cuales también han servido como parte para la organización política y la libertad para manifestarse, en virtud de que las redes sociales presentan un alto potencial para la construcción de acción colectiva ya que "reducen el tiempo, la energía y los

[56]Unión Internacional de Telecomunicaciones (UIT), *Statistics,* Dirección URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [consulta: 27 de enero, 2020].
[57]Stefano Rodotá*, op. cit.* p. 19.

recursos que los individuos dedican a discutir temas de interés colectivo, construir opinión y desarrollar propuestas"[58]

El derecho de libertad sexual también es ejercido a través de estas plataformas ya que sirven como medios para el envío de imágenes de carácter sexual o en la inscripción de redes sociales para búsqueda de pareja; inclusive derechos tan elementales como el de la salud ya que una gran cantidad de profesionales de la salud han decidido dar consultas en redes sociales como Facebook y Twitter, así como brindar información acerca de padecimientos y síntomas, así como la aparición de grupos que sirven como redes de apoyo entre personas con la misma enfermedad.

Por tal motivo, la internet se ha convertido en un fenómeno social que ha revolucionado la vida cotidiana, transformando la actuación de las personas, empresas y entidades públicas, modificado los hábitos y costumbres de ocio, laborales-profesionales e incluso la relación con el gobierno y los ciudadanos. Hoy en día, es un recurso indispensable en el desarrollo de nuestras actividades a tal magnitud que, "quien no dispone de un acceso a Internet está excluido de numerosas facetas de la vida social y económica"[59]

2.1.1 Evolución de la internet

El impacto que ha tenido y continúa teniendo internet es debido a su carácter evolutivo el cual le ha permitido una amplitud en su utilidad. Es decir, internet ha sido caracterizado por diferentes etapas, la primera de ellas denominada como "web 1.0" que hace referencia al valor técnico e instrumental de esta red para facilitar el acceso o consulta de información.

En esta primera fase la internet se caracterizaba, meramente, como un proveedor de información en el que terceros mantenían el control de acceso y grado de interrelación en la red. En esta etapa prevalecía una relación unilateral

[58] Aristeo García González, "La protección de datos personales. Derecho fundamental del siglo XXI. Un estudio Comparado", *op. cit.,* p. 69
[59] Julio César Miguel Pérez, *Protección de datos y seguridad de la información*, p. 41

con el usuario, el cual era pasivo, esto es, que "su interacción con Internet se acota a acceder o consultar simplemente información sin manifestar sus opiniones o ideas"[60]

Posteriormente, conforme avanzó la tecnología, la internet transitó de ser un modelo de información a uno también de comunicación, en virtud de que los usuarios se volvieron una comunidad activa dentro de la red gracias a la disponibilidad de nuevas herramientas (tales como dispositivos electrónicos para conectarse, conocimientos básicos del uso de la red y acceso a una conexión a internet generalizada) lo que ha permitido, hasta entonces, informarse y comunicarse entre sí además de poder crear contenidos propios.

Esta socialización de la internet refiere a una segunda etapa conocida como red 2.0, representada por una dinámica en la que los usuarios se convierten en actores receptores activos e interactivos y a la vez, en emisores productores y difusores de contenido, roles que pueden desempeñar simultáneamente, o una a la vez.

Por tanto, esta característica social de intervención de la propia sociedad hizo de Internet una gran red social en la que todos pudieran participar aportando elementos para ampliar los contenidos a través de sistemas de expresión complejos en formatos de audio, video o audiovisuales, que enriquecen los modelos de comunicación interactiva[61].

La manifestación de opiniones y posturas por parte de los internautas en una publicación de una noticia en un periódico virtual o algún otro medio informativo, o en redes sociales como Twitter o en *blogs* sobre algún tema en

[60]Lina Ornelas Núñez y Samantha Alcalde Urbina, *Ensayo 24. La protección de datos personales de menores en la era digital*, p. 19. Dirección URL:http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo24/24ensayo2014.pdf [consulta: 27 de enero, 2020].
[61]Cfr. Mariano Cebrián Herreros, "La web 2.0 como red social de comunicación e información" [en línea], p. 346 Dirección URL:http://revistas.ucm.es/index.php/ESMP/article/view/ESMP0808110345A [consulta: 27 de enero, 2019].

particular o sobre experiencias cotidianas ejemplifican este tipo de característica. Igualmente sucede con los foros de opinión en los que se intercambian ideas y apreciaciones de algún tema a debate.

Sin embargo, existe un espacio de gran significancia que ilustra este tipo de caracterización social de la internet, las llamadas "redes sociales digitales".

2.2 Redes sociales

Las llamadas redes sociales digitales, también conocidas únicamente como redes sociales, son, sin duda, el mayor impacto de la internet en la sociedad ya que su aparición, proliferación y predilección han revolucionado los esquemas tradicionales de socialización a nivel mundial[62]

En primer lugar, es conveniente señalar que una red social es definida como "una forma de interacción entre miembros y/o espacios sociales"[63]. De igual forma se señalan como "sitios en la red cuya finalidad es permitir a los usuarios relacionarse, comunicarse, compartir contenido y crear comunidades"[64]

Estas nuevas formas de comunicación social creadas por Internet permiten que los participantes puedan interactuar mediante mensajes o publicaciones públicas o privadas, compartiendo información, imágenes o videos, accesibles de forma inmediata para los usuarios.

Su origen se remonta al año 1995 con la creación del sitio web "*classmates.com*" el cual pretendía reunir a antiguos estudiantes de un colegio. Sin embargo, no fue hasta 2002 que comenzaron los sitios web que beneficiaban las redes entre amigos, tal como la plataforma de gran popularidad, *MySpace*,

[62]Cfr. Lina Ornelas Núñez, Samantha Alcalde Urbina, *op. cit.*, p. 22.
[63]Instituto Nacional de Tecnologías de la Comunicación (INTECO), Agencia Española de Protección de Datos (AEDP), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, [en línea], p. 37 Dirección URL:https://www.uv.es/limprot/boletin9/inteco.pdf [consulta: 27 de enero, 2020].
[64]Ureña, Alberto, *et al.*, *Estudio Las redes sociales en Internet* [en línea], p. 12 Dirección URL: https://www.ontsi.red.es/ontsi/sites/ontsi/files/redes_sociales-documento_0.pdf [consulta: 27 de enero, 2020].

convirtiéndose en precursora de famosas plataformas actuales como *Facebook*, *Twitter* o *Instagram*.

Actualmente, el 45% de la población mundial es usuaria de redes sociales, es decir, que 3.500 millones de personas en el mundo utilizan este tipo de plataformas[65] lo que supone un alto nivel de penetración de estas plataformas sociales en los internautas de todo el mundo, principalmente de la red social *Facebook* con 1,523 millones de usuarios diarios activos en todo el mundo lo que significa que aproximadamente un tercio de la humanidad se conecta a esta red social por lo menos una vez al mes[66]

Estas cifras no resultan fortuitas puesto que las redes sociales poseen características específicas que han propiciado su éxito ya que ofrecen una amplia interconexión mundial entre personas y la ausencia de un determinado espacio-tiempo, como servicios de la web 2.0.

En este contexto, diversos instrumentos internacionales[67] se han encargado de analizar a profundidad esta serie de particularidades que identifican a las redes sociales, las cuales se indican a continuación:

- El principal insumo para el funcionamiento de una red social es la información que los usuarios aportan al inscribirse y durante el uso del servicio, principalmente la que alude a la información de índole personal como datos de identificación, preferencias, gustos ante la necesidad de ponerse en contacto con otros individuos.

[65]We are social, *Informe Digital Around the World in 2019* [en línea]. Dirección URL: https://wearesocial.com/global-digital-report-2019 [consulta: 27 de enero, 2020].
[66]S/a, "Esta es la cantidad de usuarios que tiene Facebook en el mundo" [en línea]. Dirección URL:https://www.excelsior.com.mx/hacker/esta-es-la-cantidad-de-usuarios-que-tiene-facebook-en-el-mundo/1293579[consulta: 27 de enero, 2020].
[67]Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online emitido por la Agencia Española de Protección de Datos (AEDP) y el Instituto Nacional de Tecnologías de la Comunicación (INTECO) y el Dictamen 5/2009 sobre redes sociales en línea realizado por el Grupo de Trabajo sobre protección de datos del Artículo 29.

- Las redes facilitan la conexión e interacción sencilla, rápida y sin fronteras, desde cualquier parte del mundo y en cualquier momento. Sobrepasa el concepto, espacio y tiempo.
- Aportan herramientas que permiten a los usuarios crear su propio contenido (fotografías, mensajes, videos, enlaces, comentarios etc.) y compartirlo en línea con participantes de todo el mundo, es decir, ofrecen una base colaborativa.
- Hay una utilización de la lista de contactos de cada usuario como elemento primordial para facilitar la interconexión e interacción con otros participantes de la red social. Esta característica denota una especial relevancia ya que permite que las redes sociales lleguen a tener información de personas que no pertenecen a la misma gracias a este rasgo.
- Permiten y fomentan la posibilidad de que los usuarios inicialmente contactados a través de este medio virtual entablen un contacto real en el espacio físico.
- Tienen un crecimiento inminente basado en la difusión viral de su contenido a través de cada uno de sus participantes.

De tal forma estas características han permito que el uso de las redes sociales vaya más allá de este aspecto social para conocer personas o relacionarse con ellas, es decir, se han instituido como instrumentos democráticos para el ejercicio de la libertad de expresión y asociación respecto a situaciones de interés público que surgen en el contexto interno de las naciones, así como en contextos internacionales ante los cuales permiten expresiones de rechazo o apoyo. Del mismo modo, se han configurado como espacios de conciliación de diversas opiniones y posturas sobre situaciones en las que se violan derechos humanos, abuso de las autoridades, implementación de nuevas políticas o acciones del gobierno, etc.

Inclusive, han evolucionado para convertirse en redes de apoyo y alerta sobre situaciones más locales como grupos de alerta por la inseguridad en las

calles, testimonios de delitos o comunicar sobre el estado del tráfico. Sin embargo, a la luz de las ventajas que demuestran las redes sociales, tanto en nuestro país como el resto del mundo, sus características también potencian cuestiones negativas que se han desarrollado en estas plataformas.

Verbigracia, las redes sociales facultan convocatorias de participación a diferentes movimientos para la lucha social, pero también para convocar a actos como el linchamiento de alguien o para actos delictivos como el ocurrido en el Hidalgo, en el que se convocó para acudir al robo de combustible aprovechando la fuga que se presentaba en una de las tomas clandestinas de uno de los ductos[68].

2.3 Datos personales en las redes sociales.

Si bien y conforme a las características mencionadas, las redes sociales presentan serias implicaciones relacionadas con violación de derechos y libertades de los individuos, específicamente en el derecho a la protección de datos personales.

Lo anterior debido a que, dada la característica de acumulación masiva de datos personales en sus plataformas, dicha información de carácter personal resulta valiosa, pero a la vez peligrosa ya que existe un amplio margen para que cualquiera pueda utilizarla con fines ilícitos.

De forma que, las redes sociales, desde la perspectiva de protección de datos deben ser examinadas desde dos puntos de vista:

1) Como fuente de información en la que habremos de enfrentarnos al problema de si todos los datos personales que, de un modo u otro, aparece en la red puede ser tratada y recopilada libremente o;

[68] Verónica Ángeles, "Invitaron a todos por WhatsApp a robar gasolina en fuga de ducto", México, *El Heraldo de Chihuahua,* 20 de enero, 2019. Dirección URL:https://www.elheraldodechihuahua.com.mx/republica/invitaron-a-todos-por-whatsapp-a-robar-gasolina-en-fuga-de-ducto-2948799.html [consulta: 27 de enero, 2020].

2) Como medio para efectuar tratamientos, dado que permite recopilar, transmitir, tratar fácilmente una elevada y fácil cantidad de datos personales ya que su configuración está diseñada para que en cada conexión que se efectúe, se deje una pista que podrá ser rastreada[69]

2.3.1 Redes sociales como fuente de exposición de datos personales y medio para tratar información personal.

Si bien, la creación de las redes sociales se enfocó en una nueva forma de comunicación social en la que el principal motor es el poder compartir información y relacionarse con los demás; este aspecto se ha trasladado al terreno de la privacidad, debido a que: "las redes sociales fomentan la socialización digital y la interconectividad de las personas, teniendo esto como efecto directo la necesidad de publicar o ser visible en la red"[70], exponiendo, sin límites, todo aspecto de su persona.

Por ende, las redes sociales constituyen una gran fuente inagotable de información que emana de nuestra intimidad y vida privada y cuyo funcionamiento depende de los datos personales expresados en fotografías o videos de vivencias o amigos, datos sobre todo tipo de preferencias, ideología, experiencias, gustos, lugares frecuentes, formas de vida, formación educativa, etc.

En este sentido, el autor Byung-Chul Han (2013) analiza este fenómeno social actual desde una perspectiva de una sociedad de la transparencia cuya característica principal es la exposición. De esta manera explica que se está ante

[69]Cfr. David López Jiménez y Eduardo Carlos Dittmar, "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital", en Julián Valero Torrijos, *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, p.519

[70]Lorena Cano Orón "La privacidad en el escenario digital. Análisis de la política de la Unión Europea para la protección de datos de la ciudadanía" [en línea], Máster de Investigación en Periodismo y Comunicación, Universidad Autónoma de Barcelona, 26 de junio, 2014, p. 26. Dirección URL: https://ddd.uab.cat/pub/trerecpro/2014/hdl_2072_240336/TFM_Final_Lorena_Cano.pdf [consulta: 27 de enero, 2020].

un mundo que se ha convertido en “un mercado en el que se exponen, venden y consumen intimidades”[71].

La transparencia no sólo refiere a cuestiones políticas de rendición de cuentas y combate a la corrupción o de aspectos económicos, sino que permea en todos los aspectos del sistema social. Explica que la transparencia implica un desnudamiento voluntario sin necesidad de coacción o forzamiento para la extracción de nuestra información, “por el contrario, nos revelamos, incluso nos ponemos al desnudo por iniciativa propia”[72].

Por otro lado, la adicción que ha provocado este tipo de herramientas constituye un elemento que les impide tomar conciencia de los riesgos que pueden implicar compartir tanta información personal. Inclusive, las redes sociales se valen de las necesidades de las personas que, con el afán de ser socialmente aceptado, de ser “popular”, no sólo se comparte todo tipo de datos personales, sino que se orilla a la aceptación o confirmación para agregar a personas desconocidas que son sugeridas ante la posibilidad de ser de interés conocerlo.

Por tal motivo, se presenta un efecto en las personas que evita una reflexión sobre dicha exposición voluntaria, ya que, no surgen cuestionamientos más allá de lo que se expone, por el contrario, de aquello que no se publica es lo que genera sospecha. Ante esta situación se ignora o pasa desapercibido los alcances que puede llegar a tener esta disponibilidad de la información.

Todo dato que se expone, cada palabra, acción o actividad en la red es observado y registrado, proporcionando así una representación muy exacta de nuestra vida, de nuestra persona en un espectro digital que permite una construcción de perfiles precisos de los usuarios y presenta “al participante tan

[71]Bung- Chul Han, *La sociedad de la transparencia*, p. 68
[72]Bung- Chul Han, *Psicopolítica*, p. 62

sólo aquellas secciones del mundo que le gustan. Así se desintegra la esfera pública, critica y privatiza el mundo"[73].

Uno de los grandes cuestionamientos sobre las redes sociales es si en ellas existen o no verdaderos espacios privados libres de cualquier intromisión, sin embargo, bajo la óptica de Han, hay una preocupación de que el espacio público sufra una conversión de ser un espacio para la reflexión conjunta a un lugar de exposición, lo que supone que al existir una pérdida de lo público "se deja un vacío en el que se derraman intimidades y cosas privadas"[74]

Es decir, que la tendencia social actual de compartir intimidades y datos personales que se presenta actualmente en las redes sociales supone una privatización del espacio público que a su vez impide verdaderos espacios privados libres de intromisiones.

De esta manera, la dimensión de protección del derecho a la protección de datos personales ha sido un proceso inverso, de estar ubicado en una esfera privada, a lo largo del tiempo y con el advenimiento de los avances tecnológicos han pasado a ser consideradas de tutela pública.

Por otra parte, y derivado de la tendencia actual de exposición de datos personales en las redes sociales, surge otro aspecto primordial que debe analizarse bajo la perspectiva de protección de datos personales, las redes sociales como medio de diferentes tratamientos de información de carácter personal.

En este sentido surgen los siguientes cuestionamientos: ¿el hecho de que un dato personal proceda de una fuente de información como son las redes sociales pueden ser tratados y recopilados libremente sin el consentimiento de los titulares? ¿Hasta qué punto puede ser controlada la información personal?

[73]Bung- Chul Han, *La sociedad de la transparencia*, *op., cit.,* p. 69
[74] Ibidem.

En las redes sociales, lo que se cree que se comparte con un número reducido de personas como lo son los amigos que aceptamos para que ingresen a nuestra página o perfil social, puede ser difundido a un número incalculable de personas, perdiendo todo control sobre estos datos.

De igual forma sucede cuando creemos que sólo los usuarios de la red social a la que ingresamos pueden localizarnos o acceder a nuestro perfil, sin embargo, diversas redes sociales permiten a los buscadores de internet indexar o unir los diferentes perfiles de sus usuarios para ser localizados directamente en el buscador.

Lo anterior, trae como consecuencia que los datos personales aparezcan disponibles para que sean tratados por cualquiera, con el sólo hecho de escribir en el buscador el nombre o correo electrónico de una persona sin necesidad de inscribirse a la plataforma, a pesar de tener una configuración supuestamente privada en la red social para que nadie pueda tener acceso a información sobre nosotros.

Ante este tipo de situaciones, las redes sociales producen un cambio significativo sobre la manera en la que se accede a la información personal lo cual invita a hacer una revaloración sobre los datos personales que se proporciona a estas tecnologías.

En primera instancia, los datos de carácter personal con los que funcionan las redes sociales y que aparecen en ellas no siempre pertenecen a sus titulares, lamentablemente se pone a disposición datos de terceros, ya sean usuarios de las mismas redes sociales o inclusive no usuarios, y que en gran parte de las ocasiones no consienten esta exhibición de su información.

Es decir, cuando las publicaciones que se realizan en las plataformas sociales no se limitan exclusivamente a nosotros mismos, por ejemplo, cuando sin su consentimiento, decidimos etiquetar a amigos, familiares o conocidos o subir

fotografías o videos de ellos, y se les expone, poniendo al alcance de otros su privacidad e identidad, con gran posibilidad de que sean identificados.

Un ejemplo muy ilustrativo de esta idea es el caso de las fotografías que los padres suben de sus hijos menores de edad, en las que detallan edad, lugar al que acuden a la escuela e inclusive suelen compartir fotos de los menores desnudos o con poca ropa, lo que podría conllevar a ser fácilmente identificados a partir de esta información y ser utilizadas por terceros para fines de pornografía infantil o provocarles un daño que repercuta en el desarrollo de su vida privada o pública a una edad adulta.

Otro aspecto fundamental en el análisis de la información que se sube a las redes es que, la mayoría de los datos personales que obran en ellas pertenecen al sector poblacional que más las utilizan, los jóvenes y menores de edad. Este sector ha sido catalogado como un grupo vulnerable por su falta de experiencia, ingenuidad e inocencia que los ha llevado a ingresar todo tipo de datos sobre su persona y sobre otros, sin tener pleno conocimiento sobre la importancia de proteger su información personal y mucho menos de los peligros a los que se exponen cuando no la cuidan en este tipo de plataformas.

No es omiso mencionar que conforme evolucionan las redes sociales en sus servicios, mayor es el riesgo de entrega de datos de carácter sensible (preferencias políticas, vida sexual, nivel de ingresos, salud, datos biométricos, etc.) donde el nivel de protección y concientización por parte del usuario debería ser mucho mayor, dado que se trata de datos pertenecientes a la esfera más íntima de su vida y que podría involucrar al individuo a situaciones de grave riesgo para su integridad o someterlo a actos de discriminación.

En suma, el uso de las redes sociales implica una pérdida de control sobre los datos que se suben a ellas ya que no se puede determinar específicamente quiénes y cuántos pueden acceder a ellos y mucho menos mantener control sobre su difusión.

La disponibilidad de los datos personales en dichas plataformas sociales permite que una gama amplia de terceros interesados pueda acceder a ella de manera incontable e incontrolable. Llámense amigos o contactos que se tengan agregados en la misma plataforma, usuarios de la red social en general, desarrolladores de las redes sociales o las aplicaciones que trabajen dentro de las mismas plataformas sociales, inclusive a usuarios de otras redes sociales en vista de que sabe cuándo se empieza, pero se desconoce cuándo terminarán las intervenciones de todos los que quieran.[75]

En la actualidad una publicación en redes sociales puede volverse viral, y al suceder eso comenzará a descargarse y reproducirse infinidad de veces, incluso la publicación original podría ser modificada. Sin importar que se borre no se puede estar seguro de que ha desaparecido por completo de la red social donde se publicó o del ciberespacio, o incluso que no ha sido compartida en otras redes sociales, por lo que se pierde así el control de los datos personales del titular y los de otra persona en caso de tener el hábito de etiquetarlos.

No obstante, la falta de control que suponen las redes sociales sobre los datos personales de una persona no se limita únicamente a no saber quiénes acceden a ella, o su incontrolable difusión como ya se mencionó, sino también implica una pérdida de dominio sobre las incontables finalidades para las cuales podrían ser empleados.

Gran cantidad de casos se han registrado en los últimos años, en los que se han demostrado como se han sobrepasado los fines primarios para los que se solicitaron los datos personales y han sido utilizados indebidamente o sin consentimiento del titular, tanto por los proveedores de las mismas redes sociales como por los mismos usuarios.

Un ejemplo de ello es el uso comercial que las redes sociales hacen con la información personal de los usuarios, el cual no es consentido por los mismos.

[75] Mariano Cebrán Herreros, *op. cit.*, p.348

Esta finalidad, la cual no está prevista como el principal propósito por el cual se da el tratamiento de los datos en una plataforma de interacción social, se ha convertido en el principal motor y modelo de negocios de este tipo de servicios.

Del mismo modo, este tipo de prácticas no sólo se valen de los datos personales que los usuarios comparten, sino de datos que se generan mientras se navega en la plataforma social, los cuales también aluden a datos personales de los usuarios de las redes, como los *likes* dados a los comentarios realizados a las diferentes publicaciones; el contenido compartido, entre otro tipo de información que conforma un historial de navegación que recopilan las propias redes sociales para perfilar usuarios, vender dicha información y mostrarles publicidad personalizada.

De esta manera, es preciso señalar que los datos personales en las redes sociales como medios para su tratamiento, son facilitadores de poder[76] el cual es ejercido, no sólo por sus titulares, sino por quien los obtiene y disponen de ellos para darles el tratamiento que le plazca. Esto es que "en las sociedades informatizadas del presente, el poder ya no reposa sobre el ejercicio de la fuerza física, sino en el uso de las informaciones que permiten influir y controlar la conducta de los ciudadanos, sin necesidad de recurrir a medios coactivos"[77]

En este sentido, las redes sociales constituyen los medios por los cuales se ejercen este tipo de relaciones gracias a la extensa disposición que en ellas existe de datos de carácter personal derivado de la entrega que los internautas realizan a cada momento en dichas plataformas y el tratamiento que cualquier puede darles una vez que los obtiene o llega a ellos.

---

[76] Entendiéndose que "poder no se localiza en una esfera o institucióNn social concreta, sino que está repartido en todo el ámbito de la acción humana", Manuel Castells, *Comunicación y poder, op. cit.,* p. 39.

[77] Aristeo García González, "La protección de datos personales. Derecho fundamental del siglo XXI. Un estudio Comparado", *op. cit.,* p. 753

Esta situación constituye el riesgo principal en este ámbito ya que este trato no siempre trae beneficios para los titulares de los datos, sino que puede traer afectaciones a su persona y su entorno y a sus derechos y libertades.

El que las redes sociales sean una fuente de gran cantidad de datos personales que propician su uso masivo e incontrolable y a su vez, ser los medios por los cuales se llevan a cabo múltiples tipos de tratamientos de datos que no siempre son a beneficio del particular; resulta un gran reto en la protección de datos personales ya que en este tipo de tratamientos las fórmulas tradicionales de defensa se ven, en ocasiones, superadas o son poco efectivas.

Lo anterior debido a que las características que se presentan en estas plataformas constituyen un obstáculo fáctico y operativo que dificulta el mantener un espacio seguro para toda aquella información que los usuarios depositan en estas plataformas, lo cual les trae como consecuencia un estado de desamparo ante una serie de riesgos y afectaciones.

2.3.2. Actores involucrados en el tratamiento de los datos personales en las redes sociales

Si bien, las redes sociales tienen características implícitas que atenúan la vulneración de datos personales de los individuos, es preciso plantear a los actores responsables del tratamiento de datos personales en las redes sociales para identificar los ámbitos de actuación que tienen respecto a la problemática de la vulneración de la privacidad y datos personales de los usuarios.

Un responsable en el tratamiento de datos personales es aquel organismo público, persona moral o persona física que decide sobre el tratamiento de datos personales que obran en su posesión. En este sentido, el gobierno, los proveedores de las redes sociales, y los propios usuarios son figuras responsables de los datos personales que en ocasiones llevan a cabo prácticas que comprometen la información personal que se hallan en las redes sociales.

Los proveedores de las redes sociales son responsables del tratamiento de datos de los usuarios en virtud de que proporcionan los medios que permiten tratarlos, así como los servicios vinculados a la gestión de los usuarios, como el registro o la supresión de las cuentas.

Asimismo, son ellos los que determinan los términos sobre cómo y para qué fines serán tratados los datos de los usuarios, incluyendo los fines publicitarios o comerciales o si se les mostrará a los usuarios determinada publicidad personalizada.

Por otro lado también establecen los parámetros de seguridad y confidencialidad en la plataforma tales como la implementación del conocido diseño por defecto el cual consiste en establecer desde el diseño de la plataforma, herramientas que protejan al usuario y su información personal con configuraciones pre establecidas tales como los perfiles privados de los usuarios para, posteriormente se puedan cambiar a perfiles públicos y no viceversa como se han manejado comúnmente en los que posterior a la unión de la red social, el usuario tenga que cambiar la configuración a una privada que proteja sus datos.

Finalmente, en el caso de los usuarios, en su gran mayoría, utilizan las redes sociales en un ámbito meramente personal, es decir, para interactuar con personas de su círculo personal, familiar o doméstico resultando aplicable la denominación de *exención doméstica,* que excluye a los usuarios para figurar como responsables del tratamiento de datos personales y cumplir con el mandato de la normativa protectora en la materia.

En este orden de ideas, el entonces organismo europeo, Grupo de Trabajo Artículo 29[78] establece que la exención doméstica no será aplicada en supuestos como en los que a continuación se señalan[79]:

[78]Desde la entrada en vigor del Reglamento General de Protección de Datos Europeo, el 25 de mayo de 2018 el Grupo de Trabajo del Artículo 29 dejó de existir y ha sido reemplazado por el Consejo Europeo de Protección de Datos (EDPB) establecido en dicho ordenamiento.

1. Cuando un usuario utiliza las redes sociales en nombre de una empresa o una asociación o las utiliza como una plataforma para fines comerciales, políticos o sociales.
2. Cuando un usuario tiene un gran número de contactos terceros ya que esta situación puede indicar que no siempre que se conoce a cada uno de ellos, los cuales tienen acceso a datos de un usuario como el perfil, mensajes o historias.
3. En un criterio similar, cuando el acceso a la información del perfil de un usuario va más allá de los contactos elegidos, esto quiere decir que cuando todos los miembros pertenecientes a la red social pueden acceder a un perfil de un usuario, por ejemplo, cuando tiene la configuración de ser público. Este tipo de accesos sobrepasan el ámbito personal o doméstico, del mismo modo que si un usuario decide, conscientemente ampliar el acceso más allá de sus amigos elegidos, asume los compromisos de un responsable del tratamiento de datos.
4. La exención doméstica también aplica cuando se está ante la necesidad de garantizar los derechos de terceros, es decir, en el supuesto de que un usuario pueda ser responsable en virtud de las disposiciones generales del derecho civil o penal nacional debido a actos de difamación, responsabilidad por violación del derecho a la personalidad o responsabilidad penal.

Aunado a los diferentes actores antes señalados, es preciso resaltar el papel del Estado como juez y parte, es decir, como responsable que trata los datos y como ente que garantiza su protección.

El propio Estado, a través de sus instancias de gobierno, ha explotado los alcances que ofrecen las redes sociales para mantener contacto y relacionarse con los ciudadanos a través de perfiles o páginas gubernamentales, ya sea para

[79]Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Dictamen 5/2009 sobre las redes sociales en línea* [en línea], p. 5 Dirección URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf [consulta: 27 de enero de 2020].

gestionar la solución de dudas, quejas, asesoramiento o realización de trámites, por lo que son catalogados como responsables de los datos personales al recabarlos a través de estos medios.

Sin embargo, el Estado también tiene la obligación de garantizar las condiciones óptimas para que los tratamientos de datos personales en las redes sociales sean acordes y aseguren la protección de los derechos de los usuarios, por ejemplo, el establecer un marco regulatorio actualizado y vanguardista que contemple las regulaciones para el tratamiento de datos en este tipo de contextos digitales.

De modo que, “en las modernas sociedades tecnológicas el poder reposa en el uso de informaciones, de manera que la protección de datos personales constituye un importante criterio de legitimación política”[80] y, por ende, su reconocimiento “supone una condición del funcionamiento del propio sistema democrático”[81]

Así pues, para un óptimo funcionamiento de las redes sociales, los diferentes actores deben cumplir con la responsabilidad que la ley les obliga y respetar los derechos y libertades de los usuarios, al cumplir con los principios y obligaciones que establece el derecho a la protección de datos personales y así, cumplir con la expectativa de privacidad que tienen los mismos, que refiere a esa confianza que ellos depositan en todos los responsables involucrados en el tratamiento de su información personal que comparten al usar las redes sociales.

[80]Víctor Drummond, *op. cit.,* p. 60
[81]Ibidem.

2.3.3 Riesgos a la protección de datos personales en las redes sociales

Aunado a lo anterior, cabe señalar que 2018 fue el primer año en el que los ciberataques, el robo de datos y los fraudes cibernéticos fueron establecidos como parte de los cinco mayores riesgos mundiales a ocurrir en un plazo de diez años, de acuerdo con el "Reporte de Riesgos Globales 2018" (*The Global RisksReport*)[82] que año con año se presenta en el Foro Económico Mundial para determinar los factores de preocupación de impacto mundial.

Ésta es la primera vez que expertos identifican eventos asociados a la tecnología de la internet como factores de riesgo a nivel mundial; sin embargo, esta realidad ya no resulta del todo sorpresiva toda vez que, a lo largo del año 2018, ocurrieron diversos eventos relacionados con ciberataques de alcance mundial que dejaron muy claro su pertinencia en esta posición.

Las prácticas delictivas, fraudes o actos violentos son parte de los riesgos que se presentan en las redes sociales y que han encontrado elementos fundamentales para su difusión en internet, específicamente en las redes sociales como el lugar en el cual se pueden llegar a cometer, detectar, prevenir ante la disponibilidad de datos personales, necesaria para ser cometidos. De esta manera, el internet y las redes sociales son elementos fundamentales de la estructura de actos delictivos y delitos cibernéticos.

Asimismo, los tipos de delitos que hay en el mundo virtual de las redes sociales se distinguen por dos tipos de categorías:

1) los delitos que ya operaban en el mundo físico, pero que con herramientas tecnológicas pudieron pasar a un umbral digital, es decir, los que no

[82]Foro Económico Mundial, *The Global RisksReport 201813th Edition* [en línea]. Dirección URL: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf [consulta: 27 de enero de 2020].

son nuevos, pero se han recreado gracias a los avances tecnológicos, como los casos de fraude, robo de identidad, y otros ciberdelitos[83] y

2) los delitos que surgieron a partir del fenómeno de internet y las redes sociales.

Ahora bien, los delitos informáticos son definidos como "conductas ilícitas de acuerdo con la ley penal cometidas en contra o con la ayuda de los sistemas informáticos que pueden ser perpetradas de un lado del planeta a otro con efectos globales o locales"[84]. Su falta de fronteras; su afectación a bienes intangibles-como los datos personales e información electrónica-; así como la dificultad de comprobar el delito debido a la posibilidad del anonimato del delincuente son las principales características de su peligrosidad[85]

Los códigos maliciosos o *malwares* que se comparten a través de las redes sociales también forman parte de las herramientas que propician los delitos informáticos en las redes sociales. Este tipo de sistema es definido como "programa escrito para producir inconvenientes, destrucción, utilizar los recursos de los usuarios o recabar información de los equipos sin el consentimiento de su propietario"[86] como pueden ser los llamados virus, *spywares* o troyanos por medio de los cuales, se vulnera la información personal, en su mayoría para lograr la comisión de delitos en su contra.

Actualmente, las vulneraciones que se hacen a los datos personales en las redes sociales se expresan en una extensa cantidad de prácticas ilícitas y delitos informáticos que adquieren su principal insumo para ser cometidos en la

[83]Cfr. Carlos G. Gregorio, "Impacto y evolución de las redes sociales digitales: libertades y derechos", en Lina Ornelas y Carlos G. Gregorio (compiladores), *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes. Memorándum de Montevideo,* p. 42
[84]Alfredo Calderón Martínez, "Delito Informático: reto para los sistemas penales del mundo" en Alberto Enrique, Nava Garcés, *El derecho en la era digital. Internet, firma electrónica, protección de datos informáticos, comunicaciones, redes sociales, preservación de evidencia,* p. 3
[85] Ibid., p. 9
[86]Julio César Miguel Pérez, op. cit., p. 47

información de carácter personal; tales como los que a continuación se mencionan:

- *Grooming*: Son acciones engañosas que realiza un adulto para ganar la confianza y amistad de menores de edad, con la intención de obtener un beneficio de tipo sexual. Esta práctica es común en redes sociales ya que facilita a los adultos el acercamiento con las víctimas.
- *Cyberbullying:* Ésta es una modalidad del *bullying* o acoso escolar, pero aplicado en internet y redes sociales. Consiste en acosar públicamente a una o varias personas, las cuales padecen de diversos tipos de agresiones, entre las que se encuentran: discriminación, intimidaciones, insultos, burlas, acoso, rechazo y difamación. Los acosadores suelen ocultarse mediante personalidades falsas y suelen utilizar información de la víctima para exponerla o humillarla.
- *Ciberacoso:* Hostigamiento, humillación u otro tipo de molestias a través del móvil o del ordenador ejercido por una o varias personas durante un tiempo continuado. Control de la libertad de la víctima, una forma de violencia sobre la pareja que están adoptando muchos jóvenes.
- *Ciberamenazas:* Uso de los mensajes de correo electrónico, *SMS*, mensajes de *WhatsApp* o llamadas para infundir miedo en la víctima, para hostigarla, humillarla, para amenazarla con causarle daño (violencia física o sexual) o a sus allegados, o simplemente para molestarla.
- *Ciberextorsión:* Es una nueva modalidad de extorsión utilizando medios como las redes sociales. Puede estar relacionada con el *sexting* y consiste en obligar a la víctima a hacer cosas o dejar de hacerlas, y en muchos casos, pueden exigirle el pago de una cantidad de dinero. La persona que posee los datos personales de un individuo puede manipularlo ya que cuenta con fotografías, videos o cualquier tipo de información que no se desea que sea conocida en las redes sociales, en internet, o mucho menos a familiares o grupos de amigos.

- *Difusión de "packs":* Es el conjunto de imágenes y videos con contenido de índole sexual o eróticas, que son divulgadas en páginas o grupos de redes sociales e inclusive en páginas pornográficas ya sea por los propios titulares de las imágenes o por terceros, sin el consentimiento de su titular, para lucrar con ellas. En su mayoría este tipo de información a la que se le añaden en ocasiones datos personales extra como nombres, direcciones, lugar de trabajo o donde se estudia, entre otros, es adquirida mediante engaños en las redes sociales para ser difundidas o chantajear a través de ellas. Igualmente se ha propagado como una moda entre jóvenes por necesidades económicas o cuestiones lúdicas.

  Dicha práctica multiplica el riesgo de que los participantes pueden ser víctimas de una larga lista de delitos graves como la pornografía, trata de personas, la sextorsión, *bullying,* etc.

- *Fraudes cibernéticos:* Son engaños que utilizan medios digitales que se basan en una violación consistente a un robo de datos personales. Existen diferentes tipos de fraudes como el *phishing, pharming,* robo de identidad entre otros.

El robo de identidad es uno de los principales fraudes que se han desarrollado en la actualidad, es la utilización de datos personales de otra persona para hacerlos propios y sacar provecho de ellos por medio del engaño. Existen varios tipos de modalidades de este fraude, tal como el robo de identidad en cuestiones financieras, pero en lo que atañe a este estudio, dentro de las redes sociales también surge este tipo de fenómenos, por ejemplo, cuando alguien se apodera de un perfil o de una cuenta gracias al robo de la contraseña para que, cuanto se acceda a ella, se realicen transacciones o establecer relaciones a nombre del propietario.

Cuando un tercero roba información personal de alguien desde su perfil, como fotografías o datos en el perfil para crear con ellos una nueva cuenta con el

mismo nombre de la víctima y hacerse pasar por él y así engañar a otros y mantener relaciones con otros usuarios de manera virtual cuyas intenciones van desde las amorosas hasta las de índole de manipulación, robo de datos o dinero.

Cada una de estas prácticas, algunas ya catalogadas como delitos en algunos países, incluyendo México, son ilícitos que propician la comisión de otros delitos e incluso de delitos no necesariamente digitales, pero que ponen en riesgo la integridad de las víctimas, llevándolas a un grado de querer atentar contra su propia vida.

En este contexto, los usuarios de las redes sociales, y en ocasiones, también los que no lo son, se encuentran expuestos ante una serie de riesgos y prácticas ilícitas que se desarrollan y fortalecen en el espectro digital gracias a los datos personales disponibles en estas plataformas sociales. De esta manera, hay una afectación directa a los derechos personalísimos como la privacidad, honor, intimidad e imagen y, por ende, daño a su identidad y personalidad ligada a su dignidad y libertad como ser humano.

No obstante, el indebido tratamiento de los datos personales en las redes sociales no siempre repercute únicamente en la vida privada de las personas, sino que suelen tener también impacto en otros derechos del individuo tales como su derecho al acceso a internet y acceso a la información en virtud de que pueden estar condicionados por la obligatoriedad de entregar datos personales, aún contra su voluntad, con tal de obtener beneficios o servicios digitales, sin contar con la desconfianza de que sus datos que otorga sean ilícitamente utilizados.

Por otro lado, también se ven afectados derechos políticos como el derecho al voto libre. Un ejemplo que situó en el foco de interés público el tema de la protección de datos personales y su explotación desleal en las redes sociales fue la filtración, en 2018, de datos de 50 millones de usuarios de Facebook a la

consultora con la que trabajaba la red social, *Cambridge Analytica*, la cual utilizó dichos datos para fines electorales en las elecciones estadounidenses del 2016[87].

Este hecho evidenció la manera en la que se lleva a cabo un tratamiento indebido y no autorizado de la información personal disponible en una red social, y con un fin ajeno al establecido en los términos de la plataforma toda vez que la recolección de estos datos buscaba modificar el comportamiento de los ciudadanos para influir en su voto, lo que constituyó una clara violación a la privacidad y a la protección de datos personales de los usuarios y, por ende, una restricción a su derecho electoral de ejercer su voto libre sin ninguna clase de manipulación. A partir de entonces, la desconfianza y temor se han generalizado en gran parte del mundo.

Por lo tanto, el derecho a la protección de datos personales es un potencial derecho para vulnerar, ya que a través de él se pueden vulnerar otros derechos. Por lo que, la protección de datos es el primer paso de una garantía integral de derechos[88]

2.4 Factores de riesgo atenuantes para delitos y prácticas ilícitas en redes sociales aunado a la disposición de datos personales en las redes sociales.

Actualización del marco normativo conforme al desarrollo tecnológico.

Ahora bien, es preciso mencionar algunos factores de riesgos que propician el desarrollo de prácticas y delitos informáticos que ponen en riesgo la autodeterminación de los datos personales y la vulneración de derechos.

Un aspecto fundamental es la rápida evolución que llegan a tener las prácticas ilícitas y delitos ya que, entre más avance la tecnología, a la par los cibercriminales desarrollan técnicas y herramientas nuevas para perfeccionar, con la misma tecnología, la comisión de actividades ilícitas. Por tal motivo, ha sido

[87]Pablo De Llano, Álvaro Sánchez, "Una fuga de datos de Facebook abre tormenta política mundial", [en línea]. Dirección URL: https://elpais.com/internacional/2018/03/19/estados_unidos/1521500023_469300.html [consulta: 27 de enero, 2020].
[88]Cfr. Carlos G. Gregorio, *op. cit.,* p.45

complicado para los marcos normativos de las diferentes naciones estar vigentes ante dicha evolución continua, contrayendo deficiencias en las legislaciones.

En tal sentido, los delitos informáticos y su marco regulatorio se han convertido en un reto para las naciones y la salvaguarda de su economía, seguridad y los derechos fundamentales de los ciudadanos, ya que, si no se cuenta con una regulación o se tiene una deficiente, la situación propiciaría una gran oportunidad para los ciberdelincuentes.

Especialización para la comisión de delitos informáticos.

Consideremos ahora que los delitos informáticos pueden ser ejecutados por toda una gama de actores, desde expertos en cibercrimen como los llamados ciberdelincuentes o *hackers* a quienes definen como "alguien que irrumpe en computadoras o redes informáticas de otra persona, ya sea con fines lucrativos, de diversión o por desafío"[89]; o por cualquier otra persona sin gran cantidad de conocimientos.

Y es que, dada la gran cantidad de información personal que obra en las redes sociales, no es necesario que alguien necesite muchos conocimientos de informática para cometer algún ilícito, simplemente necesita ingresar a las plataformas, dedicar un poco de tiempo para hurgar en toda esta información y conseguir la necesaria para cometer un sinfín de malas prácticas con ella. No debe ser un experto quien quisiera irrumpir en la privacidad de un tercero, sino sólo dedicar determinado tiempo para hacer búsquedas de toda la información disponible de alguien en las redes.

Anonimato

De igual forma, el anonimato es uno de los factores de riesgo que comportan el uso de redes sociales sobre todo a cara de la privacidad y datos personales de los participantes, ya que propicia a la posibilidad de la suplantación de identidades

[89]Alfredo Calderón Martínez, *op. cit.,* p. 69

que permiten la evasión de la responsabilidad[90] sobre los actos que se realizan en estas plataformas.

Por tanto, el anonimato es un factor que atenúa que la verdadera identidad de los usuarios se ponga en duda ya que cualquiera podría presentarse en ellas con una falsa identidad, facilitando la comisión de los delitos informáticos. Es decir, en las redes sociales han germinado comportamientos inherentes a estas plataformas que en muchas ocasiones "originan un distanciamiento social ficticio, visto que la intangibilidad trae consigo una cierta insensibilidad en cuanto a la observación del otro. Por consiguiente, tienen lugar ciertas prácticas ilícitas […]"[91]

La internet ha traído como consecuencia que los usuarios desarrollen una sensación de estar protegidos por una especie de "escudo protector" constituido por la pantalla del ordenador provocando una sensación de que no pueden ser vistos por los demás usuarios, una confusión entre el mundo virtual y el real, surgiendo en ellos una impresión de autoinmunidad de no poder ser descubiertos y castigados[92].

Y es que, si bien, la dificultad de autenticar la verdadera identidad de los usuarios es una problemática presente para el combate y prevención de comisión de delitos y la aplicación de la ley en el espectro digital.

En suma, podemos resaltar que internet y las redes sociales son espacios digitales con un gran alcance para ofrecer todo tipo de servicios y mejorar la vida de las personas; sin embargo, también ha traído consigo una tendencia de la exposición de datos personales e intimidades que configura un gran riesgo para la privacidad y la protección de datos personales de las personas convirtiéndose en uno de los problemas principales del fenómeno actual que supone el internet y las redes sociales.

[90]Cfr. Carlos G. Gregorio, op. Cit., p. 44
[91]Victor, Drummond, op. cit. p. 41
[92]Ibidem.

A lo largo de este capítulo, se han desarrollado los elementos que permiten la vulneración del derecho a la protección de datos personales en las redes sociales y la manera en cómo puede afectar la esfera general de derechos de un individuo por el simple hecho de un inadecuado tratamiento de datos de carácter personal.

Por consiguiente, es dable convenir que en una sociedad democrática el desafío consiste en acentuar las tendencias y posibilidades benéficas del proceso incremental de información y conocimiento que brindan las redes sociales al tiempo de combatir con eficacia los excesos y distorsiones que inevitablemente se producen.

Para ello resulta necesario conocer, de manera general, el contexto mexicano, con el fin de identificar las áreas de oportunidad para la mejora y aprovechamiento de las redes sociales y el marco de acción en el que se debe enfocar la atención del Estado para proteger el derecho a la protección de datos personales y generar confianza en el uso de los avances tecnológicos y de negocio basados en este tipo de insumos de carácter personal.

CAPÍTULO 3. PROTECCIÓN DE DATOS PERSONALES Y REDES SOCIALES EN MÉXICO.

"Amenazar, difamar o faltar al honor a una persona en Internet no es menos delito que hacerlo en el mundo físico"

Miguel Pérez[93]

3.1 Alcance del uso de la internet y redes sociales en México.

Para comprender la protección de datos personales en México y su impacto en las redes sociales, es preciso referir a datos estadísticos que permitan conocer de manera general la situación en el país sobre la adopción y desarrollo del uso de las TIC y la penetración del uso de internet en la cotidianidad de la población mexicana.

A pesar de la brecha digital que existe en el país, a nivel urbano y rural, la posibilidad de conexión a la red de la internet se ha elevado de manera significativa en los últimos años, a la par que el número de internautas mexicanos que hacen uso de ella, tal y como se muestra en la figura 1.

Al respecto, el *15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2019*[94] arrojó que este acelerado crecimiento trajo consigo que en 2018 se registraron 82.7 millones de usuarios de internet en nuestro país, de los cuales poco más del 40% de esta población refiere a menores de edad y jóvenes de entre 6 y 24 años

En consecuencia, el grupo poblacional que conforman los menores de edad y los jóvenes representa el sector que más inmerso se encuentra en el uso de dicha tecnología y el de mayor relevancia debido a su condición vulnerable ante los riesgos que hay en su uso.

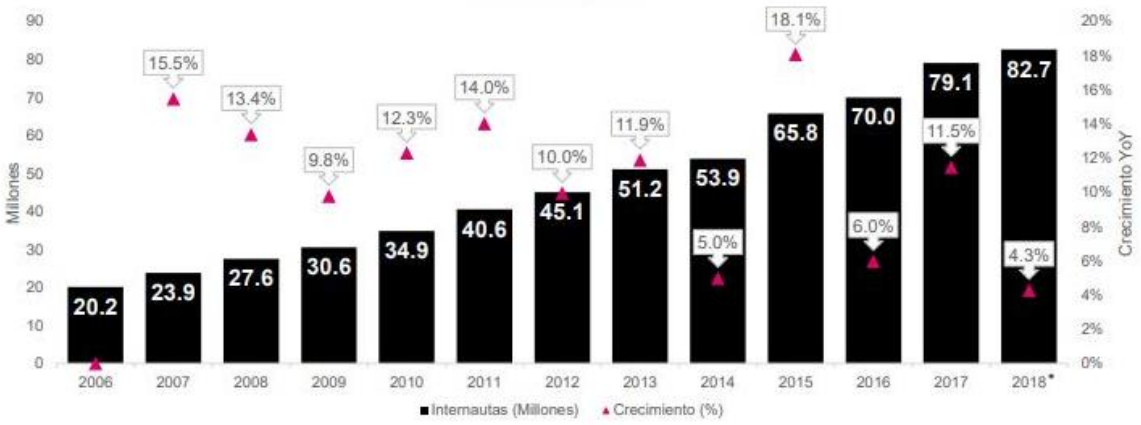
---

[93] Miguel Pérez, *op.cit.* p.63

[94]Asociación de Internet.mx*, 15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2019*, Dirección URL: https://www.asociaciondeinternet.mx/es/component/remository/func-download/97/chk,b680d989b00831d8f7fbfc68d13c37fc/no_html,1/lang,es-es/?Itemid= [consulta: 27 de enero, 2020].

Figura 1.

Usuarios de internet en México 2006-2018



Fuente: Asociación de Internet.mx, *15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*, 17 mayo de 2018.

De esta manera, si en México residen aproximadamente 125 millones de personas[95] entonces, poco más del 66% de los mexicanos son internautas que "navegan" por internet, lo cual representa que cada vez son más mexicanos que utilizan internet, dedicando poco más de ocho horas de su día a esta actividad, convirtiéndose en una práctica obligada del día a día.

Es importante mencionar que esta cifra está estrechamente relacionada con el crecimiento que se ha registrado sobre el uso de los teléfonos inteligentes, al ser el dispositivo por excelencia que los internautas mexicanos utilizan para conectarse a internet[96].

Se debe agregar que la incidencia que ha tenido el uso de internet en nuestro país se acompaña de un fenómeno de gran relevancia que son las redes sociales. El pertenecer y participar en las plataformas de las redes sociales se ha

[95]Cifra obtenida en la Encuesta Nacional de la Dinámica Demográfica, 2018, dada a conocer en el Comunicado de prensa número 337/19, 01 de julio, 2019 del INEGI. Dirección URL: https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/Poblacion2019_Nal.pdf [consulta: 27 de enero, 2020].

[96] Asociación de Internet.mx, *14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*. Dirección URL: https://www.asociaciondeinternet.mx/es/component/remository/func-download/97/chk,b680d989b00831d8f7fbfc68d13c37fc/no_html,1/lang,es-es/?Itemid= [consulta: 27 de enero, 2020].

convertido en la principal actividad en la que los internautas mexicanos invierten su tiempo al conectarse a internet, dado que el 89% de los mexicanos que se conectan a la gran red tiene predilección por esta nueva forma de socialización.

El Laboratorio de Seguridad Informática de la Facultad de Estudios Superiores (FES) Aragón de la UNAM[97] ha señalado que México ocupa el cuarto lugar en el mundo (después de Filipinas, Brasil y Argentina) con internautas que más tiempo de su día emplean para navegar en las redes sociales. Esto tiene su explicación debido a que los internautas mexicanos, de las poco más de ocho horas que dedican al día para conectarse a internet, tres horas y media son destinadas a pasar el tiempo en redes sociales.[98]

En este sentido, desde 2011, *Facebook* ha sido la red social más utilizada en el país[99], en virtud de que el 98% de los internautas la prefieren, seguida de la aplicación de mensajería instantánea *WhatsApp* con el 91%; la plataforma de videos *YouTube* tiene el tercer lugar con 82% y la red social sobre fotografías, *Instagram*, el cuarto lugar con el 57%.

En promedio, cada internauta mexicano posee cinco redes sociales y sólo el 1% no se encuentra inscrito en ninguna, lo que nos señala la importancia que tienen estas plataformas respecto con la manera en la se han posicionado como la principal actividad en el uso de internet en México.

Todo esto parecer confirmar que el uso de las redes sociales se ha popularizado en México, lo cual apunta a un escenario favorable para tener mejores condiciones de aproximación y uso de la tecnología por parte de la ciudadanía y facilitar la participación en la vida cultural y el beneficio del progreso científico y sus aplicaciones; la promoción del conocimiento, el acceso a la

[97]S/a, "México, cuarto lugar a nivel mundial en el uso de redes sociales" [en línea]. Dirección URL: https://www.excelsior.com.mx/hacker/2018/01/18/1214650 [consulta: 27 de enero, 2020].
[98]Asociación de Internet.mx*, 14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*, *op. cit.*
[99]De conformidad con información proporcionada por la Asociación de Internet.mx y cada uno de sus estudios sobre los hábitos de los usuarios de Internet en México, realizado anualmente desde 2004.

información, la participación democrática, y el ejercicio de los derechos a la libertad de expresión y de asociación, entre otros[100]

3.2 Hábitos en materia de protección de datos personales en las redes sociales en México

No obstante, como ya se ha dicho, el fenómeno de las redes sociales ha desarrollado una diversidad de nuevas conductas en los usuarios respecto a la exposición cada vez mayor de su vida privada y datos personales y México, no es la excepción.

La creciente dependencia de las tecnologías, principalmente de las redes sociales, y su elevada cantidad de usuarios ha propiciado que los internautas en el país cedan sus datos personales y luego piensen en las consecuencias que esto podría traerles, situación sumamente grave por el alto nivel de exposición para ser víctima de un sinfín de prácticas realizadas contra la persona.

Baste, como muestra que a nivel nacional el 89.4% de la población de más de 18 años tiene cuenta en alguna red social en la cual han dado a conocer sus datos personales como su nombre y apellido, seguido de su correo electrónico y su estado civil[101]. Aunado a ello, se ha demostrado que la población infantil y las mujeres adultas son quienes más utilizan las redes sociales para la publicación de fotografías de su vida cotidiana[102]

---

[100] Jacqueline L' Hoist Tapia, *Internet, tecnologías de la información y comunicación y discriminación* [en línea], p. 45 Dirección URL: https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf [consulta: 27 de enero, 2020].

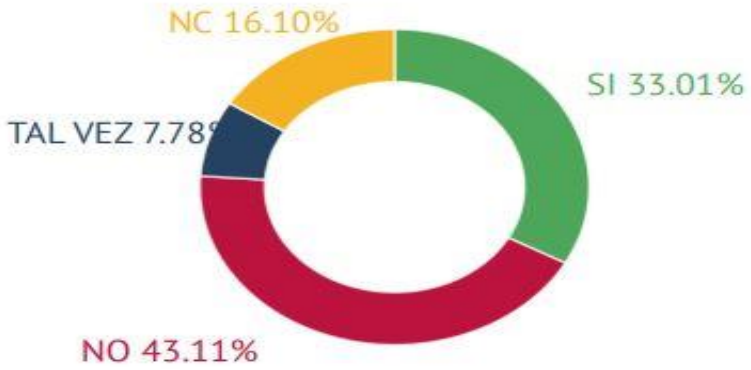
[101] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) e Instituto Nacional de Estadística y Geografía (INEGI), *Principales resultados de la Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2016 (ENAID)* Dirección URL: http://proyectos.inai.org.mx/enaid2016/images/doc/ENAID_2016_Principales_resultados.pdf [consulta: 27 de enero, 2020].

[102] Secretaría de Comunicaciones y Transportes, *Estudio Hábitos de los usuarios en ciberseguridad en México 2019* [en línea]. Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf [consulta: 27 de enero, 2020].

Por otro lado, el “Estudio Hábitos de los usuarios en ciberseguridad en México 2019”[103] indica que el compartir la ubicación dentro de las redes sociales es otra de las malas prácticas que cometen los internautas mexicanos contra su privacidad, toda vez que el 39% la aporta, lo que podría propiciar a delitos como secuestros por la identificación de los lugares que más se frecuentan

Por lo contrario, tal como se muestra en la figura 2, sólo el 33.01% de los usuarios mexicanos en redes sociales cuidan el contenido de sus fotografías antes de publicarlas, contra un 43.11% de los que han afirmado que no; el 7.78% indicó que tal vez llevan a cabo este cuidado, y el 16.10% no emitió comentarios al respecto.

Figura 2. Participantes que cuidan el contenido de sus fotografías antes de publicarlas



Fuente: Asociación de Internet.mx, *14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018*, 17 mayo de 2018.

Este tipo de problemas se intensifican si el usuario no utiliza las herramientas de configuración de privacidad que gran parte de las redes sociales ofrecen, las cuales permiten “limitar” un poco más el acceso que otros pueden tener a su información de carácter personal.

[103] Ibidem.

La Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales 2016 (ENAID)[104] realizada por el Instituto Nacional de Estadística y Geografía (INEGI) con el objetivo de estimar el conocimiento que la población mexicana tiene sobre el derecho a la protección de datos personales, ha demostrado que el 87.2% de la población de más de 18 años ha dado a conocer algún dato personal a través de una red social, quienes indicaron preocupación por el uso indebido de su información personal como su dirección o domicilio, correo electrónico, su teléfono personal, su nombre y apellidos, números de cuenta y sueldos, inclusive su currículo que contiene una serie de datos de identificación.

Esta preocupación está asociada principalmente con situaciones de acoso telefónico en el que se solicita el pago de deudas o se ofrecen servicios no solicitados, pero no así con cuestiones relativas a las redes sociales, ya que hay una creencia de que, irremediablemente se debe compartir información personal en estas plataformas, sin considerar los riesgos que implica.

Lo anterior demuestra que los mexicanos, al compartir sus datos personales, no lo hacen conscientemente ya que los comparten para obtener el servicio de la plataforma por lo que, después de haberlos proporcionados, es cuando surge un sentimiento de preocupación sobre la información difundida.

Conforme a los datos analizados, se puede observar que, en el país, los internautas mexicanos comparten inconscientemente datos personales exponiéndolos a grandes riesgos en la red, por tal motivo la popularidad de las redes sociales en el país ha venido cargada también de un alto índice de actos ilícitos, afectando la integridad de gran cantidad de ciudadanos.

En virtud de ello, la Coordinación de Seguridad de la Información de la UNAM ha revelado que, al menos 33 millones mexicanos conectados a internet,

[104]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) e Instituto Nacional de Estadística y Geografía (INEGI), *op., cit.*

han sido víctimas de algún ciberataque[105] entre los que se encuentra el intento de extracción ilegal de información de una persona, la cual puede ser de carácter personal.

Asimismo, el estudio denominado "Índice de Civilidad Digital"[106] de *Microsoft*, evaluó que México se encuentra en la posición 12 de 22 países en el que las personas están más expuestas a riesgos en línea, especialmente relacionados con temas sobre su intimidad sexual e intrusiones a su privacidad. Por consiguiente, los tres principales tipos de riesgos que más generan preocupación en los internautas de nuestro país son: 1) que alguien desconocido obtenga su información personal; 2) los riesgos relacionados con comportamientos violentos como el *cyberbullying*, ciberacoso o desprestigio; 3) situaciones concernientes a contactos de índole sexual como la sextorsión, peticiones sexuales y porno venganza.[107]

Esta preocupación no resulta fortuita, ya que el mismo estudio reveló que el 39% de los internautas confesó haber sido insultado en línea, el 36% dice haber sido ridiculizado a propósito y el 22% ha indicado que se compartió información falsa sobre ellos, mientras que el 3% restante, no dio información al respecto[108].

Por otro lado, un estudio del gobierno de México[109] reveló que el 34% de los usuarios de internet ha sufrido algún tipo de acoso de las cuales dos terceras partes son menores de edad; un 27% han sufrido robo de identidad en medios digitales, de los cuales una tercera parte son adultos; el 21% ha sufrido fraudes

[105]S/a, "33 millones de internautas mexicanos han sido víctimas de ciberataques: UNAM" [en línea], Dirección URL: https://www.eleconomista.com.mx/tecnologia/33-millones-de-internautas-mexicanos-han-sido-victimas-de-ciberataques-UNAM-20181024-0071.html [consulta: 27 de enero, 2020].
[106]Microsoft, *Civility, Safety & Interaction Online- Mexico* [en línea], enero, 2019. Dirección URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWqZ0x [consulta: 27 de enero, 2020].
[107]Ibidem.
[108]Ibidem.
[109]Estudio Hábitos de los usuarios en ciberseguridad en México 2019 Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf [consulta27 de enero, 2020].

financieros por medios digitales; el 17% extorsión por envío de fotografías de índole sexual y del 1% restante no se indicó dato al respecto.

El robo de identidad en medios digitales es uno de los actos ilícitos que más han crecido en nuestro país ya que, de acuerdo con la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), datos del Banco de México revelan que México ocupa el octavo lugar a nivel mundial en este delito[110]. Aunado a la cifra, el subdelegado de la CONDUSEF en Aguascalientes[111] informó que Facebook es la principal plataforma dentro de la cual se ha manifestado un aumento del 50% en robo de identidad gracias a la información que se comparte por esta vía relacionada con ubicaciones en tiempo real, cuentas o fechas de nacimiento, demostrando con ello, que esta red social es utilizada como mecanismo para obtener la información necesaria de la víctima para quien comete este tipo de ilícitos.

Por lo que respecta a la práctica del *sexting* o envío de información personal de carácter íntimo, como fotografías y videos de contenido sexual o erótico en nuestro país, se estima que un 34% de los internautas ha confirmado haber enviado o compartido este tipo de contenido, porcentaje en el que las mujeres representan poco más de la mitad. Sin embargo, estas cifras resultan de especial relevancia en un contexto en el que el 17% de los adultos internautas mexicanos han revelado haber sufrido extorsión por el envío de fotografías con poca o nula ropa[112]

Y es que, actualmente, la práctica del *sexting* ha sido uno de los principales detonadores de riesgos relacionados con ilícitos de carácter sexual cometidos por medio de las redes sociales, al ser llevada sin pleno conocimiento de sus

[110]Edgar Amigón, "Robo de identidad, un delito en aumento", 2015. Dirección URL: https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf [consulta: 27 de enero, 2020].
[111]S/a, "El 50% de los robos de identidad se dan por Facebook", [en línea]. Dirección URL: http://aguasdigital.com/metro/leer.php?idnota=71895&t=l [consulta: 27 de enero, 2020].
[112]Estudio Hábitos de los usuarios en ciberseguridad en México 2019 Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf [consulta: 24 de julio, 2019].

implicaciones positivas y negativas, las cuales podrían terminar en acoso e incluso trata de personas o pornografía.

En México, este fenómeno presenta un acelerado crecimiento, especialmente a nivel local, inclusive diversos estados han manifestado un alza en los casos en los que jóvenes y menores de edad, principalmente de educación de nivel básico hasta el superior, practican el *sexting* como una cuestión de moda o diversión, inclusive para obtener ganancias económicas y no así, como una nueva forma, a través de medios digitales, de poder ejercer su libertad sexual[113]

Es importante resaltar que, derivado de la práctica del *sexting*, en nuestro país ha surgido un fenómeno con gran auge mejor conocido como el envío de "packs". Esta práctica al igual que el *sexting,* se centra en compartir conjuntos de fotografías con contenido sexual o erótico, la cual se desarrolló entre la comunidad de estudiantes de nivel secundaria y media superior entre 2016 y 2017[114]

A diferencia del *sexting,* el envío de *packs* se presenta de tres maneras distintas para la adquisición de este tipo de contenidos, una en la que el propio titular de las imágenes las comparte en redes sociales para la obtención de popularidad o por necesidad de pertenencia, o ya sea para comercializar con ellas al solicitar, a cambio de compartirlas, determinadas cantidades de dinero.

Otra forma en la que opera esta modalidad sucede cuando terceros roban fotografías de otras personas que yacen en los perfiles de redes sociales, para ofrecerlas en grupos o páginas —ya sea dentro o fuera de la misma plataforma social—, con el fin de comercializarlas al ofrecer servicios sexuales o para lucrar con ellas. En esta modalidad, frecuentemente los delincuentes acuden a engaños o fraudes dentro de la misma plataforma para convencer a las víctimas y obtener

[113]S/a, "Al alza practica del sexting en Quintana Roo" [en línea], Dirección URL: https://laverdadnoticias.com/quintanaroo/Al-alza-practica-del-sexting-en-Quintana-Roo-20180418-0050.html [consulta: 27 de enero, 2020].
[114]S/a, "Hacer "packs" incrementa riesgo de acoso escolar y delitos, advierten" [en línea], México, *televisa.news,* 19 de agosto, 2018. Dirección URL: https://noticieros.televisa.com/historia/hacer-packs-incrementa-riesgo-de-acoso-escolar-y-delitos-advierten/ [consulta: 27 de enero, 2020].

las imágenes de tipo sexual, las cuales, una vez obtenidas, son utilizadas para extorsionar al titular con que serán difundidas y así adquirir más.

Esta situación se expresa en la estadística del país toda vez que el 30% de cibernautas mexicanos han revelado haber recibido peticiones persistentes no deseadas para enviar imágenes íntimas suyas o de otros[115]

Finalmente, en lo que refiere a la tercera forma en la que se obtienen o recolectan este tipo de imágenes de índole sexual, sucede cuando la víctima comparte las fotografías o videos íntimos voluntariamente con alguna persona de su confianza como su pareja, o cuando permite que ésta sea quien las tome. El problema surge cuando este último actor, posteriormente, rompe el lazo de confianza al difundirlas en redes sociales u otras formas digitales como chats de mensajería instantánea.

La exposición de nuestra información personal, especialmente en datos de índole sexual, han situado a los internautas mexicanos ante situaciones de pérdida de su privacidad sexual, afectaciones a su estado emocional o a ser víctima de extorsión, fraude, secuestro y trata de personas, entre otros crímenes.

A pesar de las cifras expuestas, no existe cifras claras sobre el número de casos de esta naturaleza cometidos en las redes sociales ya que muchos de ellos no se denuncian o no proceden ante su falta de tipificación como delitos; por tanto, resulta evidente la existencia de un rezago en medidas jurídicas para perseguir y castigar responsables de ataques cibernéticos, así como la falta de preparación de los Ministerios Públicos respecto a estas nuevas modalidades de “delitos”, el seguimiento de los casos y el análisis respectivo.

[115]Microsoft, *Civility, Safety & Interaction Online- Mexico*, *op., cit.*

3.2.1 Ejemplos de vulneración de datos personales en redes sociales en México

Aunado a lo anterior, en México, los ejemplos abundan en cuanto a la relación entre el uso de redes sociales como medio para llevar a cabo una violación a los datos personales. Derivado de su trascendencia mediática se hace referencia del caso de la estudiante del Estado de Puebla llamada Olimpia Coral Meno, quien, en 2012, cuando tenía 18 años, accedió a que su pareja grabara un video en el momento en que mantenían relaciones íntimas, el cual fue difundido por el mismo, llegando al grado de ser explotado en internet a nivel mundial por al menos seis páginas pornográficas.

A raíz de la difusión, la joven fue objeto de burlas en redes sociales donde la bautizaron con diversos sobrenombres, además de ser víctima de extorsiones por parte de las páginas pornográficas ya que le solicitaban una suma de dinero como pago para eliminar el video de sus sitios web.

El acoso sufrido por parte de la víctima la llevó al intento de suicidio tres veces, sin embargo, en 2013 impulsó una iniciativa para tipificar como delito la difusión de imágenes, vídeos y textos de contenido sexual, ante el Congreso del Estado de Puebla. No obstante, fue hasta diciembre de 2018 cuando finalmente se aprobó la reforma al Código Penal del Estado de Puebla, en la que se tipificó como delito de violación contra la intimidad sexual, con castigo de cárcel, a quien suba a Internet imágenes, videos y audios de contenido sexual difundidos sin el consentimiento de todos los involucrados.

Asimismo, en 2017, fundó la organización llamada Frente Nacional para la Sororidad enfocada al combate de la violencia en redes sociales, la cual ha impulsado diversas reformas en este sentido, en diferentes estados del país.

En circunstancias similares, una joven del Estado de Veracruz, Ana Baquedano, también fue víctima de la difusión de información íntima sobre su

persona a la edad de 16 años, ya que una de sus fotografías en la que aparecía semi-desnuda se hallaban circulando en Facebook.

La fotografía fue difundida por su exnovio sin su consentimiento, por lo que fue objeto de burlas y humillaciones. Posteriormente su imagen apareció junto con su información de contacto en una página web dedicada a exhibir fotografías de jóvenes que obtenía vía Facebook.

A pesar del acoso sufrido, Ana, junto con otras instituciones, logró que, en 2018, se aprobara una reforma al Código Penal del Estado de Querétaro para reconocer como delito contra la imagen personal la "pornovenganza", que consiste en la difusión, revelación, publicación, o exhibición, sin su consentimiento, de imágenes, texto y grabaciones de contenido erótico o sexual a través de publicaciones en redes sociales o cualquier otro medio.

Por tal motivo, fue acreedora en agosto del mismo año al Premio Estatal de la Juventud 2018[116], por su labor social para impulsar una nueva norma que castigara este tipo de actos de violencia, así como por su labor de alertar a las mujeres y hombres en el estado, sobre temas de acoso y hostigamiento.

Finalmente, uno de los casos más recientes fue el relacionado con los Cadetes del Colegio Militar y la Fuerza Aérea Mexicana presentes en la toma de protesta del actual presidente Andrés Manuel López Obrador y la divulgación de sus datos personales a través de las redes sociales.

Durante la toma de protesta presidencial, los usuarios de redes sociales comenzaron a emitir una serie de comentarios sobre los dos cadetes presentes en el acto al grado de llegar a ser identificados rápidamente por los mismos usuarios, quienes se dieron a la tarea de investigar la identidad de estos jóvenes y compartirla a través de algunos datos como sus nombres, edades, lugares de

[116] S/a, "Galardón a jóvenes por su aporte a la sociedad" [en línea]. Dirección URL: https://www.yucatan.com.mx/merida/galardon-jovenes-aporte-la-sociedad [consulta: 27 de enero, 2020].

origen, fotografías, videos, su perfil de *Facebook* y *Twitter*, incluso la relación amorosa de uno de ellos.

La reacción de las personas ante esta información fue tal que saturaron las cuentas de redes sociales de los jóvenes con la gran cantidad de solicitudes de amistad que les fueron enviadas. Aunado a lo anterior, diversos medios de comunicación también difundieron este tipo de datos sin el consentimiento de los jóvenes y sin considerar su derecho a la privacidad al agregar en sus notas informativas algunos de los datos que fueron revelados.

Ahora bien, por lo que respecta al primer y segundo caso, ambos son situaciones con gran similitud ya que los perjuicios que se presentaron en ambas víctimas fueron a consecuencia del uso redes sociales para la difusión de datos personales con fines violentos contra su sexualidad, así como un medio por el cual, se han llegado a crear mercados para comercializar con esta información.

En ambos ejemplos se actualizaron situaciones de "pornovenganza", "sextorsión", ciberacoso y *cyberbullying*, así como una clara violación a sus derechos de imagen de cada víctima y a su reputación y honor, dañando su dignidad e integridad humana.

También demuestran claramente como el hecho de compartir nuestra información aún a personas de nuestra "confianza" podría llevarnos a esta clase de situaciones toda vez que, al exhibir cuestiones tan íntimas de nuestra persona, datos especialmente sensibles y de suma protección, nos deja en un estado de indefensión e impotencia y se brinda a terceros poder sobre nosotros.

Esta situación no es casual ya que en México el 44% de los riesgos en línea a los que están expuestos los internautas provienen de personas cercanas o de su confianza[117], como familiares, amigos o pareja.

[117]Microsoft, *Civility, Safety & Interaction Online- Mexico*, *op., cit.*

Por lo que refiere al tercer caso, aunque fue un hecho que se volcó humorístico, la realidad es que estos jóvenes cadetes fueron víctimas de la práctica denominada *doxing* debido a que fueron objeto de investigación acerca de su vida privada para después, hacerla pública sin su consentimiento a través de la difusión de su información de carácter personal la cual, a pesar de que yacía en las redes sociales, era de índole privado.

Aunado a ello y como en los casos anteriores, se ilustra una situación de ciberacoso, en el que los cadetes recibían una gran cantidad de solicitudes de información, así como una intromisión a su vida privada que ellos no habían consentido.

Si bien, en este caso y hasta el momento, la difusión de los datos personales no ha llegado a consecuencias graves que atenten contra los cadetes como en los casos anteriores; sí se da cuenta de una situación que exacerbó los riesgos que pueden tener la divulgación de tanta información concerniente a su persona a causa de su condición de miembros de instituciones de seguridad pública.

Esta serie de casos demuestran la facilidad con la que se pierde el control de nuestra información una vez que decidimos compartirla bajo la creencia de confianza y sin pensar en las posibles consecuencias, asimismo, se demuestra que, en todas las situaciones, las finalidades para las cuales se comunica inicialmente nuestra información difieren radicalmente cuando algún tercero dispone de ella y la utiliza para objetivos desproporcionales e ilegítimos.

A su vez, un factor primordial en este tipo de actos es el factor de anonimato de quien reproduce o trata inadecuadamente la información personal ya que no siempre se le identifica. Si bien, la información está en plataformas sociales, en las que incluso podrían haber estado con una configuración abierta al público, no significa que existe la condición para disponer de los datos de los demás y difundirlas a gran escala sin respetar ni proteger los derechos ajenos.

Es posible rescatar que las publicaciones de imágenes de carácter sexual o eróticas, tanto las que son compartidas voluntariamente como las que no lo son, es una práctica que va al alza en nuestro país afectando a gran parte de la población de jóvenes y mujeres.

Su importancia se ha materializado en un auge de propuestas de reforma normativas en diferentes estados de la República en los que se han aprobado o sometido para su aprobación ya sea en sus Códigos Penales o Leyes de Acceso a las Mujeres a una Vida Libre de Violencia estatales para tipificar como delitos el ciberacoso, la pornovenganza, la violación a la privacidad sexual como violencia digital o la tipificación de delitos informáticos como la recolección de información personal sin el consentimiento del titular, entre otros; para regular la protección a la privacidad sexual de las mujeres ante vulneraciones a su espacio íntimo por el uso inadecuado de los datos personales.

En definitiva y conforme a los datos antes expuestos, se propone señalar la necesidad de considerar internet y las redes sociales como espacios de interacción social y desarrollo personal en los que se exponen dinámicas sociales que eventualmente pueden lesionar los derechos de los ciudadanos. Sin embargo, también constituyen espacios de oportunidad para la prevención y difusión de una cultura en materia de protección de datos personales.

Participar en esta nueva era digital, debe estar acompañada de una conciencia de la importancia que tiene la huella digital que se deja en el ciberespacio y la manera en la que se puede evitar ser víctima de todas las situaciones antes mencionadas, de ahí la importancia de crear conciencia en los ciudadanos sobre el uso de estas herramientas tecnológicas.

3.3 Cultura de protección de datos personales en el espacio de interacción social de las redes sociales

El problema actual de la vulneración de datos personales derivado de su exposición en las plataformas de redes sociales no radica completamente en los desarrolladores de los aparatos móviles, ni en los medios de transmisión de los datos como son las redes sociales, sino que se comparte con la cultura actual de quienes interactúan en el espacio digital y el modo en el que manipulan las herramientas que suponen las redes sociales para la interacción social.

Por tal motivo resulta primordial definir que, de acuerdo con el autor Manuel Castells (2009) cultura es "el conjunto de valores y creencias que dan forma, orientan y motivan el comportamiento de las personas"[118], de esta manera, la cultura es un modo de vida y una forma de convivencia, es la formación de una concepción para ver la vida y para actuar sobre ella[119]. Sin embargo, es preciso abordar este término desde un contexto del ciberespacio en el que se desarrolla el presente estudio, por lo que se evocará al término "cultura digital".

La cultura digital refiere a "la cultura propia de las sociedades en las que las tecnologías digitales configuran decisivamente las formas dominantes tanto de información, comunicación y conocimiento como de investigación, producción. organización y administración"[120].

Por lo tanto, cultura digital refiere a las actitudes, valores y formas de pensar que se desarrollan en el ciberespacio, en esta misa debe imperar lo respectivo a la cultura en materia de protección de datos personales con el objetivo de determinar una conciencia sobre este derecho, sus prácticas y formas de actuar con base en sus principios y deberes fundamentales para crear un modo de vida y una forma de convivencia que reconozca la importancia y el valor que

[118] Manuel Castells, *Comunicación y poder*, p. 65
[119] Javier Esteinou, "Cultura para la sobrevivencia", en Francisco Blanco Figueroa, *Cultura y globalización*, p. 189.
[120] Pierre Lévy, *Cibercultura: La cultura de la sociedad digital*.

tiene la información personal para el respeto y ejercicio de los derechos de la persona y de tercero.

Por tal motivo, uno de los elementos primordiales en el espacio de interacción social que suponen las redes sociales es la difusión y fortalecimiento de una cultura de la protección de datos personales ante los gravámenes que la exposición de datos personales y los riesgos de ser utilizados inadecuadamente pueden contraer a los ciudadanos digitales. En este sentido, la cultura de protección de datos se refiere al "conjunto de conocimientos, opiniones, prácticas o conductas que una persona tiene sobre el tratamiento y la protección de su información personal (datos personales)"[121]

De lo anterior Aristeo García (2013) indica que la cultura de protección de datos personales debe atender a una doble acepción: un aspecto jurídico (conocimientos) y desde un aspecto social (opiniones, prácticas o conductas).[122]

Por lo que concierne al enfoque jurídico, el autor señala que no basta con dar a conocer a la población la existencia de un marco normativo en materia de protección de datos personales, es necesario que también conozcan el derecho desde sus componentes esenciales como lo son sus principios rectores y su contenido, su reconocimiento como prerrogativa fundamental, la figura del responsable y el organismo garante de la protección del derecho; así como su relación con otros derechos, es decir, "tiene que proyectarse en la forma en cómo se debe entender y enseñar la cultura jurídica en materia de protección de daos"[123]

Desde un enfoque social, la cultura de protección de datos refiere a dar a conocer no sólo el tránsito de la protección de datos personales en el ámbito

[121] Aristeo García González, "Hacia una cultura en materia de protección de datos personales" [en línea], Dirección URL: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4971 [consulta: 27 de enero, 2020].
[122] Ibidem.
[123] Aristeo García González, "Hacia una cultura en materia de protección de datos personales", *op., cit.*

jurídico, sino dar a conocer la nueva etapa de la vida social influenciada por el creciente uso y desarrollo de la tecnología. Esto es, la perspectiva social "se encuentra regida por las opiniones, prácticas o conductas que cada día expresamos en las redes sociales, tales como pensamientos, sentimientos, comentarios, fotografías y videos de nuestro quehacer cotidiano"[124], situación que afecta la propia privacidad de la sociedad.

Conforme a lo anterior, el enfoque social refiere a una perspectiva de la conducta social, y a "efectos de entender este nuevo entorno de comunicación y expresión, es preciso decir que, los individuos actúan siguiendo determinados patrones de conducta transmitidas socialmente" tal como la exposición completa de su vida privada en las redes sociales como ya se explicó anteriormente.

Bajo este entendido, es preciso ahondar en la cultura en materia de protección de datos personales que puede vislumbrase en la relación de los internautas mexicanos con el derecho a la protección de datos y el conocimiento que tienen sobre la normativa, y su actuar en el contexto del uso de las redes.

3.4 Cultura de protección de datos personales en México.

3.4.1 Nivel de conocimiento sobre el derecho a la protección de datos personales en México

Ejercicio del derecho a la protección de datos personales

De acuerdo con la Encuesta Nacional de Percepción Ciudadana realizada por el INAI en 2018, de 2,100 entrevistas efectivas a nivel nacional de hombre y mujeres mayores de 13 años, el 74% ha escuchado sobre el derecho a la protección de datos personales[125] y el 85% cree que todos los mexicanos tienen derecho a la protección de su información personal.

---

[124] Ibidem.

[125] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda). Reporte de Resultados, [en línea]. Dirección URL: http://inicio.inai.org.mx/Estudios/inai_parametro_201_v7.pdf [consulta: 27 de enero, 2020].

De igual forma el 84% han indicado que sienten mucha preocupación sobre la protección de sus datos personales y un promedio del 40% han mencionado mucha preocupación por su información personal, principalmente por la divulgación de datos como domicilio, teléfono, número de tarjeta bancaria, huella dactilar, CURP, RFC y número de seguridad social. No obstante, consideran que cuando han sido violados sus datos personales en su gran mayoría no hacen nada al respecto porque desconocen lo que pueden hacer o no saben con quién acudir.

Estas cifras contrastan respecto al 86% que ha señalado que nunca ha ejercido su derecho a la protección de sus datos de carácter personal debido a que, en su mayoría, creen que no han tenido la necesidad de hacerlo, seguido de personas que no sabe cómo hacerlo o que no ha tenido el interés ni el tiempo o porque no conocían el derecho.

Este mismo estudio indicó que el 13% de los encuestados ha ejercido su derecho a la protección de datos personales y ha sido derivado del hecho de que:

1) ha sufrido acoso telefónico,

2) busca evitar que hagan mal uso de sus datos,

3) porque ya han hecho mal uso de su información personal,

4) por haber sido víctima de extorsión y robo de identidad.

Por otro lado, cabe señalar que el marco normativo en materia de protección de datos personales actualmente prevé cuatro derechos en los que se hace efectivo el derecho de protección de datos, los derechos ARCO. Al respecto, el estudio en comento señala que poco más del 50% de los encuestados tienen conocimiento sobre ellos, pero en su gran mayoría no los utilizan.

Aunado a lo anterior, el marco normativo también prevé un canal de denuncia ante afectaciones a los datos personales de una persona por actos de un organismo público o una entidad privada; o en su caso, para que cualquier

persona que conozca de situaciones en las que se esté incumpliendo dichas disposiciones pueda denunciar este tipo de hechos. No obstante, el estudio en comento señaló que en 2018 sólo el 5% de los encuestados, a nivel nacional, habían presentado una queja por el uso indebido de datos personales, de los cuales sólo el 36% acudió al INAI para presentar la denuncia[126].

Lo anterior demuestra que son pocas las personas que ejercen su derecho a la protección de datos personales a través de este medio y ante el órgano nacional garante de este derecho, debido a que prefieren acudir a instituciones gubernamentales como la CONDUCEF o a la Procuraduría Federal del Consumidor (PROFECO).

Este tipo de cifras denotan que en el país existe un conocimiento vago o poco claro del derecho que protege la información personal, sin embargo, también existe una actitud positiva hacia el cuidado sobre este tipo de información lo que podría ser aprovechado para fortalecer y desarrollar una verdadera conciencia acerca del derecho a la protección de datos personales a través de incentivar la educación en este derecho y con ello contrarrestar la desconfianza ante un mal uso.

Conocimiento de mecanismos y/o vías para el ejercicio del derecho a la protección de datos personales

Los mexicanos comparten sus datos personales de manera inconsciente con el fin de obtener beneficios de diversos servicios y posteriormente sentir preocupación por la información difundida, sin embargo, tanto internautas como los que no lo son, desconocen los mecanismos mínimos prescindibles para proteger sus datos ante la angustia de su difusión, por ejemplo, el conocer y leer un Aviso de Privacidad.

[126] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda). Reporte de Resultados, *op. cit*.

El Aviso de Privacidad cobra un carácter primordial para el derecho estudiado, en virtud de que es el medio por el que se brinda información a las personas sobre qué datos sobre su persona tratará una entidad pública o privada, cómo, porqué y para qué serán utilizados y cuál será el tratamiento al que estarán sujetos sus datos personales. Una vez que se tiene toda esta información, la persona puede dar un consentimiento informado para que sean utilizados conforme a los fines necesarios para brindar el servicio siempre que sean proporcionales y no excesivos.

Empero, en 2018, a nivel nacional, este mismo estudio indicó que sólo el 22% de los encuestados ha manifestado que se les ha dado a conocer un Aviso de Privacidad, de los cuales, únicamente el 23% ha leído alguno[127]. Esto evidencia que 1) el porcentaje de los mexicanos que tiene conocimiento de la existencia de los Avisos de Privacidad es sumamente bajo y 2) aunado al bajo porcentaje existente, también hay un nivel de atención bajo a este tipo de documentos, ya que, de los pocos mexicanos familiarizados con el instrumento, son pocos los que lo leen o atienden cuando está disponible.

Lo anterior brinda una aproximación de que los mexicanos dan sus datos sin siquiera saber para qué y cómo serán utilizados y de qué manera se llevara a cabo su tratamiento, agotando así uno de los elementos mínimos que les puede dar un nivel de certeza y confianza de saber de qué manera estarán protegidos y que aspectos deben atenerse.

En virtud de lo anterior, resalta la necesidad de un sentido autodidacta y de responsabilidad única de los ciudadanos para prestarle mayor atención e interés a este mecanismo que busca la procuración de la seguridad y protección de los datos personales.

[127]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda). Reporte de Resultados, *op. cit*.

Otro aspecto importante que reflejó dicho estudio fue el desconocimiento del derecho de datos personales, en el entendido de que sólo la mitad de los encuestados han escuchado o conoce el marco normativo en la materia de protección de datos personales[128], en este sentido, quienes si conocen de la regulación ha indicado que el conocimiento que han adquirido, en su mayoría, ha sido a través de la televisión, seguido del Internet y la radio[129]

Por lo que respecta al conocimiento sobre el organismo garante del derecho a la protección de datos personales, el INAI, se evidenció que poco menos del 50% identifica que existe una institución a nivel nacional encargada de la protección de este derecho, de los cuales el 66% califica como muy buena su labor, atribuyéndole como una de sus principales funciones la protección de sus datos personales, sin embargo, a pesar de tener una opinión positiva del mismo, tampoco se tiene pleno entendimiento sobre sus funciones y cómo sirve a la ciudadanía.

Percepción sobre los riesgos y violaciones de los datos personales

Por otro lado, la percepción de seguridad que tienen los mexicanos sobre sus datos personales en los servicios de redes sociales es sumamente baja ya que perciben un nivel de seguridad del 4, cuando 10 es muy seguro y 1 muy inseguro[130].

Asimismo, los ciudadanos asocian como parte de los principales abusadores de sus datos personales, a las empresas privadas, las plataformas de redes sociales, partidos políticos, o el propio gobierno[131]; no obstante, las personas no consideran el grado de responsabilidad que recae en ellos al

[128]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda). Reporte de Resultados, *op. cit*.
[129]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) e Instituto Nacional de Estadística y Geografía (INEGI), *op., cit*.
[130]Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda). Reporte de Resultados, *op. cit*.
[131]Ibidem.

proporcionar su información personal y la de terceros sin tener conciencia de su valor intrínseco.

De tal forma, en México, ante los riesgos a la privacidad y datos personales en las redes sociales, los ciudadanos reaccionan más desconfiados de otras personas en línea, así como de personas que no están en un medio digital tornando su vida se vuelve más estresante.

En mérito de lo expuesto, se prevé un existente, pero bajo nivel, de conocimiento sobre el derecho a la protección de datos personales en México, en el cual predomina la confusión, desconocimiento y poca cultura.[132] Si bien, los mexicanos conocen de la imperiosa necesidad de proteger los datos personales de carácter personal, no existe un pleno conocimiento sobre que es un derecho reconocido no sólo a nivel internacional, sino que es un derecho fundamental[133] que brinda las prerrogativas para la defensa y protección de los datos personales en el país.

Conforme a lo establecido para analizar la cultura de protección de datos respecto a un aspecto jurídico, se demuestra que no hay conocimiento del marco jurídico ni de sus particularidades para poder ejercer el derecho satisfactoriamente y con un mínimo de protección, como es el conocimiento del propio derecho, del Aviso de Privacidad o del INAI como canal para proteger y auxiliar a los titulares de los datos personales.

De esta manera hay una proyección de que la forma en cómo se está entendiendo el derecho y cómo se enseña esta cultura jurídica en materia de protección de datos personales está siendo insuficiente y preocupante al trasladarlo al ámbito digital y sus ilimitadas y desregularizadas fronteras.

---

[132] Ibidem.

[133] Un derecho fundamental tiene como base un derecho humano, sin embargo, el primero está reflejado y plasmado en un texto constitucional y aplicado en un territorio nacional. Oscar Armando González Vega, "Derechos humanos y derechos fundamentales" [en línea], Dirección URL: https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/12556/14135 [consulta: 27 de enero, 2020].

Asimismo, tanto en las cifras estadísticas como en los ejemplos anteriores, se proyecta el otro aspecto que se debe analizar bajo una perspectiva de cultura de protección de datos, el aspecto social que refiere a la forma en la que la comunicad digital se comporta en las redes sociales, comportamiento regido por opiniones, prácticas o conductas expresadas en las redes sociales.

Las estadísticas evidencian que la popularización e incremento de uso de las redes sociales, a las que cada vez más tienen más acceso los mexicanos, viene acompañada de un fenómeno en el que se ha identificado una diversidad de nuevas conductas y actitudes en la población de usuarios contrarias al cuidado y seguridad de datos personales ya que es tanta la necesidad de estar conectados y pertenecer a un mismo círculo social a través de las redes sociales que los usuarios en el país no se detiene a pensar en las consecuencias que implica la vulneración a su privacidad y datos personales.

En este sentido, en México se han manifestado malas prácticas y actitudes en este sentido, respecto a sus datos personales y a los de terceros, inclusive se ha dado muestra de prácticas ilícitas mencionadas a lo largo de este capítulo en algunos ejemplos de casos que han sido resonados y que hay marcado pauta sobre cómo los propios usuarios violentan los datos personales que obran en las redes sociales y las consecuencias que este tratamiento ilícito ha traído consigo.

Esta problemática hay que plantearla desde dos supuestos: cuando se es el titular de los datos y no hay conciencia sobre su propia información personal y sus derechos; y en el supuesto en el que no se tiene conciencia sobre la protección de los datos de otros, llámense amigos, familiares, pareja, conocidos o terceros ajenos.

Así pues, hoy se registra un sentimiento de inmunidad al estar detrás de una pantalla que inhibe cualquier responsabilidad sobre el respeto al derecho ajeno; de igual forma, estamos ante una realidad en la que parece que cada vez es más necesario exponer y compartir datos personales y tratar esta información

disponible en la red para finalidades que llegan a grados altos de vulneración de la dignidad e integridad de las personas.

En este sentido, Javier Esteinou (2001) plantea que a pesar del fenómeno que representa la posibilidad de acumulación de información en las redes sociales como nunca antes se había visto, los niveles de humanización no avanza de igual manera, entendiéndose como niveles de humanización a que la persona sea más comprensiva hacia los demás, hacia su entorno y con quienes convivimos; al contrario, se da un mayor individualismo, por tanto mayor intolerancia y menor respeto de otros para conservar niveles de sobrevivencia básicos que requerimos para existir[134]

En esta lógica, ante el fenómeno de desmaterialización que se produce a través de las redes sociales como consecuencia de circunstancias como el anonimato, falsas identidades, etc., que han facilitado la perfección de actos contra las personas a partir de su información personal, el principal actor para que este tipo de situaciones cese, es el usuario.

Si bien, son distintos los actores que pueden trastocar los derechos a través de las redes sociales y de la vulneración de datos personales, tanto las empresas privadas como las mismas plataformas sociales son intervinientes sobre la actividad en línea y quizá su objetivo principal en estos medios y en sus prácticas no es necesariamente el apoyo al ejercicio de los derechos, sino a generar beneficios económicos.

Por tanto, el impacto sobre el derecho a la protección de datos queda en manos de agentes con intereses distintos a la protección del usuario por lo que los riesgos provenientes de las prácticas de este tipo de actores tal como el uso comercial oculto y sin consentimiento de los usuarios a partir de los datos personales que generan, pueden ser combatidos desde una perspectiva del

[134]Crf., Javier Esteinou, "Cultura para la sobrevivencia", *op. cit.,* p. 182

usuario, al disminuir los datos personales que se proporcionan o utilizando los mecanismos de privacidad para sopesar los riesgos de que sean mal utilizados.

Los usuarios resultan ser un factor sumamente importante para contrarrestar los fenómenos delictivos que se han desarrollado en las plataformas sociales a partir de un conocimiento pleno de sus derechos y una cultura fortalecida sobre la protección de datos en el ámbito digital. Por lo tanto, hace falta fortalecer el derecho y no dejar que se quede en un conocimiento a medias que tergiverse el sentido principal de esta prerrogativa.

De poco sirve tener un marco normativo sólido e incluso instituciones garantes que defiendan derechos fundamentales en específico la protección de datos personales, si en la realidad el derecho no cobra arraigo entre las personas, y a partir de ellas, adquiera una forma y volumen suficiente para hacerlo exigible; es decir, “la supervisión sobre el impacto de internet en un marco normativo que garantice los derechos discurre en dos sentidos: en las posibilidades de usar internet para los derechos y en la forma en que ese ejercicio es fácticamente posible”.

Es preciso trabajar en la creación de una conciencia clara sobre la protección de datos personales y el ejercicio de la privacidad que se tiene en las redes sociales y en todo el entorno digital, debido a que, como sociedad es importante atender estos problemas ya que no sólo nos afecta como individuos, sino como comunidad.

Como sociedad, se deben de apreciar las tecnologías derivadas de internet bajo una base de conductas éticas y de servicio público, así como mediante los análisis que den evidencia de sus riesgos de forma imparcial y objetiva con la

finalidad de potenciar sus bondades reales de emancipación y de progreso civilizatorio[135].

De igual forma, “conocer los rasgos de una sociedad resulta imprescindible para dilucidar cómo es posible estar a la altura de las exigencias morales que ella misma plantea”[136]. Estas exigencias se concretan en la necesidad de fomentar el protagonismo de los ciudadanos como dueños de la vida pública digital a través de la concientización y cultura respecto al cuidado de sus datos personales y por ende, de su espacio privado, el cual resulta una condición necesaria para el ejercicio de su libertad individual.

En esta lógica, urge pues que el Estado, a través de sus instituciones aborden el tema desde la educación y la cultura ya que constituye la fuerza más poderosa para impulsar en el país una verdadera cultura en la protección de datos personales y diseñar aquellas medidas que pueden fortalecer la ciudadanía en vez de debilitarla, enfrentando la problemática desde una perspectiva social con base en los propios usuarios.

Lo anterior bajo el entendido de que el Estado es el encargado de proteger los derechos de sus miembros en los cuales se encuentran inmersas sus relaciones económicas, políticas y sociales en el nuevo espectro digital. Por lo tanto, resulta imprescindible que el gobierno enfoque sus acciones y políticas públicas tomando en consideración la protección de datos personales desde una perspectiva de fomento a la cultura de protección de datos personales en el ámbito digital, para no dejar en estado de vulnerabilidad a los individuos.

Es decir, la actualización de las acciones gubernamentales en materia de protección de datos deberá estar dirigida al fortalecimiento de una conciencia, educación y cultura en protección de datos personales de la sociedad para

---

[135] Mucio Israel Hernández Guerrero, “Privacidad y datos personales en internet” [en línea], p. 25. Dirección URL: https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf [consulta: 27 de enero, 2020].

[136] Adela Cortina Orts, “Ciudadanía activa en una sociedad mediática”, en Jesús Marcial Conill Sancho y Vicent Gonzálvez (coordinadores), Ética de los medios, p. 17

garantizar en internet un espacio seguro con elemento mínimos que protejan las acciones y relaciones de los individuos en este ámbito y permitan el libre ejercicio de sus derechos.

No se trata sólo de una arquitectura normativa y de la emisión de políticas en papel, se trata del involucramiento de un elemento humano en el conocimiento de la protección de datos personales en virtud de que constituye el eslabón inicial por el cual se puede garantizar la protección de su vida y su libertad en el nuevo espacio digital; en virtud de que, es la persona quien desarrolla su vida en este ámbito, ejerce sus derechos, toma las decisiones día a día sobre su protección y seguridad digital.

CONCLUSIONES

Como se desarrolló a lo largo del presente trabajo, nuestra vida se ha trasladado cada vez más al espectro digital, el cual se ha convertido en un espacio donde se conjunta la interacción social. No obstante, de manera proporcional al crecimiento del uso de internet y las redes sociales, aumentan los riesgos y las amenazas en este ámbito, propiciados por un inadecuado tratamiento de datos personales, los cuales son cada vez más lascivos a la persona y a su esfera de derechos toda vez que es un nuevo espacio en el que se ejercen sin dilación las libertades y derechos de los ciudadanos.

Retomar las redes sociales desde una perspectiva en materia de protección de datos personales expone la existencia de una importancia creciente y autónoma del derecho a la protección de datos personales como un elemento básico para el uso y ejercicio de los derechos a través de dichos medios tecnológicos.

Como se advirtió, la protección de datos personales es un derecho que brinda a los individuos una capacidad de actuación positiva sobre toda su información personal, que le permite mantener control y poder sobre ella y a su vez proteger y respetar sus derechos y su libertad individual como rasgo principal de la dignidad humana, en un nuevo espacio de debate e interacción social que instauran las redes sociales.

Asimismo, el abordar la protección de datos personales en las redes sociales, expone un tema de relaciones de poder, toda vez que los datos personales constituyen facilitadores de poder, no sólo para su titular, sino para quienes los obtienen, ya que al tratarlos y disponer de ellos como les plazca, pueden influir, controlar o dañar al titular o terceros, a través de tratamientos ilegítimos, ilegales y perjudiciales para sus derechos y libertades.

De esta manera, su protección adquiere relevancia al servir como elemento fundamental para el combate y prevención de los riesgos, delitos y malas prácticas que son llevadas a cabo a través de estos medios contra los titulares o terceros involucrados.

El proteger en el espectro digital de las redes sociales el derecho a la protección de datos personales también incentiva a que otros derechos pueden ser ejercidos libremente —con independencia de otros factores que puedan menoscabar a la par estos derechos—, es decir, es un derecho habilitador de otros derechos.

Por lo tanto, la protección de datos personales es un atenuante para que un individuo tenga el poder de ejercer sus derechos y adquiera la confianza de que su identidad y todo lo que concierne a su persona estará protegida y por ende podrá manejarse con libertad en su desarrollo privado e íntimo, así como en su desenvolvimiento como ser social en el ámbito digital.

Para ejercer esta capacidad de actuación efectiva que brinda el derecho a la protección de datos personales en las redes sociales, es necesario que exista una cultura de protección de datos en los ciudadanos que utilizan y que no utilizan estas herramientas, para atender el desconocimiento del derecho que los protege, así como mitigar la proliferación de diversas prácticas y conductas delictivas generadas por las características de las redes sociales.

No obstante, el presente análisis arrojó que el grado de madurez de la cultura de la protección de datos personales en México, apenas alcanza los mínimos deseables, en virtud de que la mayor parte de la población 1) no tiene noción del valor de sus datos personales, especialmente de su valor económico y 2) a pesar de que, en ocasiones conoce o le resulta familiar el derecho a la protección de sus datos personales, ignora sus implicaciones y alcances y por ende no lo ejerce con libertad y plenitud.

Este panorama resulta más agravante cuando se traslada a un ámbito digital como las redes sociales que presenta el fenómeno de la cada vez mayor exposición de datos personales tanto de internautas como de los que no lo son, convirtiéndose con ello en una de las mayores fuentes para la extracción ilícita de datos personales, a la vez que sirven como el principal medio para su tratamiento ilegal, propiciando la proliferación de diversas prácticas y conductas delictivas que dejan vulnerable a la sociedad ante la delincuencia digital.

Inclusive, se advirtió que la incalculable disposición de los datos personales en las redes sociales debido a la poca cultura en la materia ha permeado en discusiones de interés, como la dicotomía de lo público y lo privado respecto al fenómeno de la disolución de lo público ante la cada vez mayor publicidad de la intimidad y la privacidad.

En este sentido el problema no radica en las redes sociales propiamente, sino en el uso que las personas hacen de ella. De esta forma, nos enfrentamos no sólo a un desconocimiento de la importancia y el valor de los datos personales y su derecho de protección, sino a una sociedad que ha sido inherentemente influenciada por una cultura en la que prevalece el interés por mayores niveles de acumulación de bienes económicos, traspasándose al espectro de las redes sociales para volverlas una fuente de ganancias a costa de la afectación de una persona y de la vulneración de sus derechos, cualesquiera que estos sean.

De igual forma hay una crisis en cuestión de valores éticos en el uso de las tecnologías que inciden en la violación de los datos personales y la privacidad, así como en la propagación de diversas prácticas y conductas delictivas que dejan vulnerable a la sociedad ante la delincuencia digital y malas prácticas en ella.

Conforme a lo anterior, se ha identificado como punto principal de atención , los usuarios de las redes sociales. El tema de una cultura de protección de datos personales, desde una perspectiva digital y dirigida al usuario, es un tema actual, inminente y crucial que requiere un rol activo del Estado para la creación y aplicación de políticas enfocadas a una cultura de prevención más que de

mitigación, así como trabajar en el fomento de los derechos ciudadanos que, debido a las nuevas tecnologías, ahora están siendo vulnerados.

De esta manera, la protección de los datos personales ha adquirido una dimensión social de gran importancia decisiva, que obliga una doble intervención, la del Estado mexicano y la de la sociedad.

El Estado tiene la obligación de cuidar de los intereses colectivos, la seguridad y los derechos de las personas al buscar un fortalecimiento mayor de la cultura ciudadana en las redes sociales, toda vez que los usuarios constituyen el eslabón débil de la cadena de protección de los datos en las redes sociales, por lo que el enfoque de este derecho debe dirigirse a la ciudadanía y fortalecer su protagonismo como dueños de la vida pública digital, a través de una colaboración del Estado hacia la sociedad.

De esta manera, el Estado a través del poder público, debe impedir que poderes privados, en este caso, tanto los desarrolladores de las redes sociales, empresas publicitarias, pero principalmente, los usuarios de las redes sociales se abstengan de hacer pública la vida privada y la intimidad de las personas a través de la exposición de los datos personales a través del ahínco de acciones preventivas enfocadas a la sociedad.

Asimismo, es necesario que el propio usuario adopte su parte responsiva sobre su información y la de terceros que obren en su poder, y hagan uso de sus derechos humanos respetando los derechos de los demás ya que ningún gobierno, grupo o persona individual tiene derecho a actuar en detrimento de los derechos de los demás.

Para garantizar un nivel alto de protección de los derechos y libertades de las personas se requiere un nivel uniforme y elevado de conocimiento del tema de protección de las personas con respecto a su información personal que responda a las necesidades y exigencias actuales, y que a su vez no establezca barreras a

la libre circulación de los datos personales para el desarrollo económico y las actividades comerciales del país.

Un aspecto mínimo necesario para evitar agresiones en el espacio digital es la existencia de un marco normativo adecuado relacionado con el ámbito mediático y la protección de su información personal en ella. En México, esto ya se materializa en la normativa de protección de datos personales, que si bien, la Ley Federal de Protección de Datos Personales en Posesión de Particulares no está del todo actualizada conforme a los avances tecnológicos y los tratamientos que ya surgen a través de las redes sociales, si existe un margen de protección que no deja en indefensión a los ciudadanos respecto a la protección de sus datos de carácter personal.

Aunado a este déficit que presenta la legislación en la materia, el fenómeno que constituyen las redes sociales, específicamente con respecto a la exposición masiva de información personal y la prevención, las leyes no son del todo suficientes. Es necesario un conocimiento de la norma, así como una educación sobre este derecho que permita fortalecer una cultura en materia de protección de datos personales, así como valores éticos que dirijan el uso de los medios digitales.

Por lo tanto, se aboga por buscar nuevas formas auto regulatorias de la sociedad en las redes sociales que coadyuven con el fortalecimiento de los sistemas normativos a partir del desarrollo y priorización de una cultura de protección de datos personales desde la dimensión jurídica, es decir, el fortalecimiento del conocimiento del marco jurídico para poder ejercer el derecho satisfactoriamente y garantizar un mínimo de protección; así como en el aspecto social relativo al actuar sobre el comportamiento manifestado en el uso de las redes sociales.

México se posiciona ante un gran reto respecto a la apertura y consolidación del derecho a la protección de datos personales en el uso de las redes sociales para construir un escenario, en el ámbito digital, que haga del

ejercicio del derecho a la protección de datos algo fácticamente posible a través del fortalecimiento de una cultura ciudadana en materia de protección de datos personales de los internautas mexicanos.

El apego de México en acuerdos internacionales como el Convenio 108, la normativa en protección de datos vigente para el sector privado y el público, así como el contar con un órgano garante del cumplimiento y protección de este derecho como lo es el INAI, son indicadores que ofrecen certeza de la obligación que el país ha contraído a nivel mundial relativo a la implementación del derecho a la protección de datos personales en su derecho interno, sin embargo debe ser fortalecido con una mayor cultura de protección de datos que socialice el derecho en la comunidad.

La protección de datos personales es un derecho que debe ir madurando y para lograrlo es importante e imprescindible una socialización del derecho para que pueda ser ejercido y que se consagre como una herramienta para protegerse en el espectro digital.

No se debe olvidar que el actuar del Estado democrático mexicano constituye el instrumento efectivo de protección del derecho a la protección de datos personales incluidas las redes sociales, como condición preventiva y necesaria para el ejercicio de las libertades (personal, de pensamiento, de expresión, entre otras), las cuales constituyen el núcleo de las libertades democráticas toda vez que, la democracia se expresa y se construye sobre las libertades y derechos de los ciudadanos.

Por tal motivo, resultaría conveniente retomar el derecho a la protección de datos personales a través de una actualización del marco normativo y la implementación de políticas públicas y acciones gubernamentales en la materia, pero desde una perspectiva de las tecnologías actuales. Asimismo, realizar especial énfasis en iniciativas educativas que fortalezcan la cultura de protección de datos y que favorezcan, a su vez el uso responsable y cívico de las nuevas

tecnologías en coadyuvancia con políticas en materia de digitalización, acceso a la información y de acceso a internet.

Las redes sociales no deben convertirse en espacios que propicien muestras de odio y violencia entre sus usuarios, no deben terminar siendo herramientas que violen la privacidad y protección de datos personales de los usuarios, sino deben ayudar a promover libertades personales, comunicación entre sus miembros, promover la participación más que el miedo y la incertidumbre.

Para ello se requiere de una nueva lógica en el tratamiento de los datos personales en el ámbito digital de las redes sociales que tome en cuenta la educación, concientización, socialización y elaboración de todo un andamiaje para la sociedad con el fin de proteger su vida, libertad, sus relaciones políticas, económicas y sociales, así como sus derechos, no sólo en el uso de las tecnologías actuales sino que sirvan como punto de partida ante tecnologías y prácticas venideras que podrán traer mayores retos al respecto.

REFERENCIAS BIBLIOGRÁFICAS

Amigón, Edgar, “Robo de identidad, un delito en aumento” [en línea], México, *Revista Proteja su Dinero*, CONDUSEF, Núm. 186, 2015, Dirección URL: https://www.condusef.gob.mx/Revista/PDF-s/2015/186/robo.pdf

Andreu Martínez, María Belén y María Carmen Plana Arnaldos, “El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico”, en Julián Valero Torrijos, *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica,* España, Editorial Thomson Reuters Aranzadi, 2013*,* pp. 131-151.

Ángeles, Verónica, “Invitaron a todos por WhatsApp a robar gasolina en fuga de ducto” [en línea], México, *El Heraldo de Chihuahua,* 20 de enero, 2019. Dirección URL:https://www.elheraldodechihuahua.com.mx/republica/invitaron-a-todos-por-whatsapp-a-robar-gasolina-en-fuga-de-ducto-2948799.html

Araujo Carranza, Ernesto, *Derecho a la Información y la Protección de Datos Personales en México*, México, Porrúa, 2009, pp. 33-12.

Arcos, Eduardo, “El inspirador discurso de Tim Cook en la Universidad de Stanford: «Sean diferentes, dejen al mundo creaciones que tengan valor»” [en línea], México, *Hipertextual*, 17 de junio, 2019. Dirección URL: https://hipertextual.com/2019/06/inspirador-discurso-tim-cook-universidad-stanford-sean-diferentes-dejen-mundo-creaciones-que-tengan-valor

Asociación de Internet.mx*, 14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018* [en línea], México, 17 mayo, 2018. Dirección URL:https://www.asociaciondeinternet.org.mx/es/component/remository/func-startdown/81/lang,es-es/?Itemid=

Asociación de Internet.mx*, 15° Estudio sobre los Hábitos de los Usuarios de Internet en México 2019* [en línea], México, 01 agosto, 2019. Dirección URL: https://www.asociaciondeinternet.mx/es/component/remository/func-download/97/chk,b680d989b00831d8f7fbfc68d13c37fc/no_html,1/lang,es-es/?Itemid=

Calderón Martínez, Alfredo, "Delito Informático: reto para los sistemas penales del mundo" en Alberto Enrique Nava Garcés, *El derecho en la era digital. Internet, firma electrónica, protección de datos informáticos, comunicaciones, redes sociales, preservación de evidencia,* México, Porrúa, 2013, pp. 1-14.

Cano Orón, Lorena, "La privacidad en el escenario digital. Análisis de la política de la Unión Europea para la protección de datos de la ciudadanía" [en línea], Máster de Investigación en Periodismo y Comunicación, Universidad Autónoma de Barcelona, 26 de junio, 2014, pp. 46. Dirección URL: https://ddd.uab.cat/pub/trerecpro/2014/hdl_2072_240336/TFM_Final_Lorena_Cano.pdf

Cashmore, Pete, "Privacy is dead, and social media hold smoking gun" [en línea], México, *CNN*, 28 de octubre, 2009. Dirección URL: https://edition.cnn.com/2009/OPINION/10/28/cashmore.online.privacy/

Castells, Manuel, *Comunicación y poder*, Madrid, Alianza Editorial, 2009, pp. 65

Castells, Manuel, "Internet, libertad y sociedad; una perspectiva analítica" [en línea], *Polis. Revista Latinoamericana,* núm. 4/2003, 19 de octubre, 2012. Dirección URL: http://journals.openedition.org/polis/7145

Cebrián Herreros, Mariano, "La web 2.0 como red social de comunicación e información" [en línea], Madrid, *Estudios sobre el Mensaje Periodístico,* Universidad Complutense de Madrid, *vol. 14, 2008, pp. 345-361.* Dirección URL:http://revistas.ucm.es/index.php/ESMP/article/view/ESMP0808110345A

Charvel Orozco, Sofía," Bienvenida", en H. Cámara de Diputados, *Protección de Datos Personales. La voz de los actores*, México, Tiro Corto Editores, 1ª ed., 2001, 13-14.

Cortina Orts, Adela, "Ciudadanía activa en una sociedad mediática", en Jesús Marcial Conill Sancho y Vicent Gonzálvez (coordinadores), *Ética de los medios,* España, Gedisa, 2004, pp. 11-31

D. Vargas, César, *La globalización del e-gobierno y la transparencia de la información pública*, España, Delta Publicaciones, 2011, pp. 177

De Llano, Pablo y Álvaro Sánchez, "Una fuga de datos de Facebook abre tormenta política mundial", [en línea], Estados Unidos, *El País,* 20 de marzo, 2018. Dirección URL:https://elpais.com/internacional/2018/03/19/estados_unidos/1521500023_469300.html

Drummond, Víctor, *Internet, Privacidad y Datos Personales,* Madrid, Editorial Reus, 1ª ed., 2004, pp. 172

Escalante Gonzalbo, Fernando, *El derecho a la privacidad,* México, Colección Cuadernos de Transparencia/IFAI, 1ª ed., 2008, pp. 43

Esteinou, Javier, "Cultura para la sobrevivencia", en Francisco Blanco Figueroa, *Cultura y globalización*, México, Dos siglos, Dos Milenios, Excelencia y Futuro 2, Universidad de Colima, 1ª ed., 2001.

Foro Económico Mundial, *The Global RisksReport 2018, 13th Edition* [en línea], Ginebra, 2018. Dirección URL: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf

Fundación Kaleidos**,** *Proximidad en el ámbito local. Proximidad, nuevas tecnologías y participación ciudadana en el ámbito local*, España, TREA, 2010, pp. 20-25

G. Gregorio, Carlos “Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América Latina” en Sergio López Ayllón, *et al. Transparentar al Estado: la experiencia mexicana de acceso a la información*, [en línea], México, UNAM, Instituto de Investigaciones Jurídicas, 2004. Dirección URL: https://archivos.juridicas.unam.mx/www/bjv/libros/3/1407/12.pdf

G. Gregorio, Carlos, “Impacto y evolución de las redes sociales digitales: libertades y derechos”, en Lina Ornelas y G. Gregorio Carlos (compiladores), *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes. Memorándum de Montevideo,* México, Instituto de Investigación para la Justicia (II Justicia), Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), 1ª ed., 2011, pp. 41-73

García González, Aristeo, “La protección de datos personales. Derecho fundamental del siglo XXI. Un estudio Comparado”*,* [en línea], México, *Boletín Mexicano de Derecho Comparado*, Instituto de Investigaciones Jurídicas, año XI, núm. 120, septiembre-diciembre, 2007, Dirección URL: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4971

García González, Aristeo, “Hacia una cultura en materia de protección de datos personales” [en línea], México, *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas, núm. 14, 2013. Dirección URL: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3933/4971

García Ricci, Diego, *El derecho a la privacidad*, México, Nostra Ediciones, 2017, pp. 68.

Garriga Domínguez, Ana, *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua,* Madrid, Editorial Dykinson, 1ª ed., 2016, p.20-50

Garzón Valdés, Ernesto, *Lo íntimo, lo privado y lo público*, México, Colección Cuadernos de Transparencia/IFAI, 2005, pp. 47

Gómez, Gallardo, Perla, *Libertad de expresión, protección y responsabilidades*. [en línea], Ecuador, Editorial Quipus, CIESPAL, 2009, Capítulo 3, pp. 145-225. Dirección URL: http://biblio.flacsoandes.edu.ec/catalog/resGet.php?resId=55166

González Vega, Oscar Armando, "Derechos humanos y derechos fundamentales", [en línea], México, *Revista Hechos y Derechos*, Instituto de Investigaciones Jurídicas, núm. 45, mayo-junio 2018. Dirección URL: https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/12556/14135

Grimalt Servera, Pedro, "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y solapamientos con otros derechos y libertades en internet", en Julián Valero Torrijos, *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica,* España, Editorial Thomson Reuters Aranzadi, 2013, pp. 65-87

Grupo de Trabajo sobre Protección de Datos del Artículo 29, *Dictamen 5/2009 sobre las redes sociales en línea,* [en línea], adoptado el 12 de junio, 2009. Dirección URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_es.pdf

Han, Byung-Chul, *La sociedad de la transparencia,* España, Herder Editorial, 1ª ed., 2013, pp. 96

Han, Byung-Chul, *Psicopolítica,* España, Herder Editorial, 1ª ed., 2018, pp. 127

Hernández Guerrero, Mucio Israel, "Privacidad y datos personales en internet" [en línea], *Revista Dfensor – El uso de las nuevas tecnologías y los derechos humanos*, Comisión de Derechos Humano del Distrito Federal, núm. 6, año XIV,

junio 2016, pp. 22-28 Dirección URL: https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf

Hernández, Juan Carlos, “La protección de datos personales en Internet y el habeas data” [en línea], Venezuela, *Revista Derecho y Tecnología*, núm. 13, enero/diciembre, 2012, Centro de Investigaciones en Nuevas Tecnologías de la Universidad Católica del Táchira, pp. 61-85. Dirección URL http://www.corteidh.or.cr/tablas/r32012.pdf

Herrán Ortiz, Ana Isabel, *La violación de la intimidad en la protección de datos personales*. España, Editorial Dykinson S.L, 1999, pp. 414

Instituto Nacional de Tecnologías de la Comunicación (INTECO) y Agencia Española de Protección de Datos (AEDP), *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online* [en línea], Madrid, febrero 2009, Dirección URL: https://www.uv.es/limprot/boletin9/inteco.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Encuesta Nacional de la Dinámica Demográfica*, 2018, dada a conocer en el Comunicado de prensa número 337/19, 01 de julio, 2019 del INEGI. Dirección URL: https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/Poblacion2019_Nal.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI), *Encuesta Nacional de Percepción Ciudadana, INAI 2018 (Estudio de opinión cuantitativo, cara a cara en vivienda)*. *Reporte de Resultados,* [en línea], México, noviembre 2018. Dirección URL: http://inicio.inai.org.mx/Estudios/inai_parametro_201_v7.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI) e Instituto Nacional de Estadística y Geografía (INEGI), *Encuesta Nacional de Acceso a la Información Pública y Protección de Datos Personales*

2016 (ENAID)-Principales resultados [en línea], México, octubre, 2006. Dirección URL:http://proyectos.inai.org.mx/enaid2016/images/doc/ENAID_2016_Principales_resultados.pdf

L' Hoist Tapia, Jacqueline, *Internet, tecnologías de la información y comunicación y discriminación* [en línea], *Revista Dfensor – El uso de las nuevas tecnologías y los derechos humanos*, Comisión de Derechos Humano del Distrito Federal, núm. 6, año XIV, junio 2016, pp. 42-47 Dirección URL: https://cdhdf.org.mx/wp-content/uploads/2016/09/dfensor_06_2016.pdf

Lévy, Pierre, *Cibercultura: La cultura de la sociedad digital*, Barcelona, Antrophos-Universidad Autónoma Metropolitana (UAM)-Iztapalapa, 2007, pp. 256

López Jiménez, David y Eduardo Carlos Dittmar, "Internet móvil y geolocalización: nuevos retos para la privacidad en la era digital", en Julián Valero Torrijos, *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica,* España, Editorial Aranzadi, 2014, pp. 519-542

Luengo López, A., "Adicción a Internet: conceptualización y propuesta de intervención" [en línea], España, Revista Profesional Española de Terapia Cognitivo-Conductual, ASETECCS, núm. 2, 2004, pp. 22-52. Dirección URL: http://www.jogoremoto.pt/docs/extra/BL5L6u.pdf

Microsoft, *Civility, Safety & Interaction Online- Mexico* [en línea], enero, 2019. Dirección URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWqZ0x

Miguel Pérez, Julio César, *Protección de datos y seguridad de la información*, México, Editorial Ra-Ma, 4ta ed., 2015, pp. 272

Nieves Saldaña, María, "The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis" [en línea], España, *Revistas Científicas de la UNED*, núm. 85,

2012, pp. 195-239. Dirección URL: http://revistas.uned.es/index.php/derechopolitico/article/download/10723/10242

Ornelas Núñez, Lina y Samantha Alcalde Urbina, *Ensayo 24. La protección de datos personales de menores en la era digital*, México [en línea], México, Colección Ensayos para la transparencia de la Ciudad de México, Instituto de Acceso a la Información Pública del Distrito Federal (InfoDF), mayo de 2014, pp. 91.DirecciónURL:http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo24/24ensayo2014.pdf

Peschard Mariscal, Jacqueline, "El derecho fundamental a la protección de datos personales en México" en José Luis Piñar Mañas y Lina Ornelas Núñez (coordinadores), *La protección de Datos Personales en México,* México, Tirant lo Blanch, 2013, pp. 19-38

Piñar Mañas, José Luis y Lina Ornelas Nuñez, "Los principios de la protección de datos personales" en José Luis Piñar Mañas y Lina Ornelas Nuñez (coordinadores), *La protección de Datos Personales en México,* México, Tirant lo Blanch, 2013, pp. 39-95

Rodotá, Stefano, "Democracia y protección de datos" [en línea], España, Instituto Nacional de Administración Pública (INAP), *Cuadernos de Derecho Público*, números 19-20, 2003, pp. 15-26 Dirección URL: https://revistasonline.inap.es/index.php?journal=CDP&page=article&op=view&path%5B%5D=690

S/a, "33 millones de internautas mexicanos han sido víctimas de ciberataques: UNAM" [en línea], México, *eleconomista.com,* 2 de octubre, 2018. Dirección URL: https://www.eleconomista.com.mx/tecnologia/33-millones-de-internautas-mexicanos-han-sido-victimas-de-ciberataques-UNAM-20181024-0071.html

S/a, “Al alza practica del sexting en Quintana Roo” [en línea], México, *La Verdad,* 18 de abril, 2018. Dirección URL: https://laverdadnoticias.com/quintanaroo/Al-alza-practica-del-sexting-en-Quintana-Roo-20180418-0050.html

S/a, “El 50% de los robos de identidad se dan por Facebook” [en línea], México, *aguasdigital.com,* 06 de marzo, 2018. Dirección URL: http://aguasdigital.com/metro/leer.php?idnota=71895&t=l

S/a, “Esta es la cantidad de usuarios que tiene Facebook en el mundo” [en línea], *Excelsior.com*, 30 de enero, 2019. Dirección URL: https://www.excelsior.com.mx/hacker/esta-es-la-cantidad-de-usuarios-que-tiene-facebook-en-el-mundo/1293579

S/a, “Galardón a jóvenes por su aporte a la sociedad” [en línea], México, *Diario de Yucatán,* 12 de agosto, 2018. Dirección URL: https://www.yucatan.com.mx/merida/galardon-jovenes-aporte-la-sociedad

S/a, “Hacer “packs” incrementa riesgo de acoso escolar y delitos, advierten” [en línea], México, *televisa.news,* 19 de agosto, 2018. Dirección URL: https://noticieros.televisa.com/historia/hacer-packs-incrementa-riesgo-de-acoso-escolar-y-delitos-advierten/

S/a, “México, cuarto lugar a nivel mundial en el uso de redes sociales” [en línea], México, *Excelsior.com,* 18 de enero, 2018, Dirección URL: https://www.excelsior.com.mx/hacker/2018/01/18/1214650

Secretaría de Comunicaciones y Transportes, *Estudio Hábitos de los usuarios en ciberseguridad en México 2019* [en línea], México, 2019. Dirección URL: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

Sitio web oficial de la Organización de los Estados Americanos (OEA), “Sobre e-Gobierno”, [en línea]. Dirección URL:

http://portal.oas.org/Portal/Sector/SAP/DepartamentoparalaGesti%C3%B3nP%C3%BAblicaEfectiva/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx

Solange Maqueo Ramírez, María, Barzizza Vignau, Alessandra, Democracia, privacidad y protección de datos personales, México, Instituto Nacional Electoral - número, Cuadernos de divulgación de la cultura democrática, 41, 1ª ed, 2019, pp.7-69

Unión Internacional de Telecomunicaciones (UIT), *Statistics*, Dirección URL: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Ureña, Alberto, *et al.*, *Estudio Las redes sociales en Internet* [en línea], Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI), diciembre 2011. Dirección URL: https://www.ontsi.red.es/ontsi/sites/ontsi/files/redes_sociales-documento_0.pdf

Villanueva, Ernesto, "Derecho a la vida privada", en Ernesto Villanueva, *Derecho de la Información. Conceptos básicos,* Ecuador, Editorial *Quipus*, CIESPAL, 2003, pp. 233-240.

We are social, *Informe Digital 2019,* [en línea], 2019. Dirección URL: https://wearesocial.com/global-digital-report-2019

Instrumentos Normativos Internacionales

Convención Americana sobre Derechos Humanos suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos (b-32) San José, Costa Rica, 7 al 22 de noviembre de 1969, Convención Americana sobre Derechos Humanos (Pacto de San José) [en línea]. Dirección URL: https://www.oas.org/dil/esp/tratados_B32_Convencion_Americana_sobre_Derechos_Humanos.pdf

Convenio Europeo de Derechos Humanos, [en línea]. Dirección URL: https://www.echr.coe.int/Documents/Convention_SPA.pdf

BIBLIOGRAFÍA

Araujo Carranza, Ernesto, *Derecho a la Información y la Protección de Datos Personales en México*, México, Porrúa, 2009, pp. 33-12.

Barindelli, Florencia, "Género e Internet", en Lina Ornelas y Carlos G. Gregorio (compiladores), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, Instituto de Investigación para la Justicia (IIJusticia) e Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), 1ª ed., México, 2011. pp. 127- 159.

Bauzá Reilly, Marcelo, "La protección de datos personales y su armonización con otros derechos y las políticas de gobierno", en Álvaro Sánchez Bravo, *Derechos humanos y protección de datos personales en el siglo XXI: homenaje a Cinta Castillo Jiménez,* España, Punto Rojo Libros, 2014, pp. 53-77.

Cerdio, Jorge, "*Alcances de la reforma al artículo 16 constitucional"*, en H. Cámara de Diputados, *Protección de Datos Personales. La voz de los actores,* México, Tiro Corto Editores, 1ª ed., 2001, pp. 27-33.

Díaz Buck, Anid Vanessa, "La autorregulación en redes sociales como forma de garantizar los derechos de intimidad, privacidad y protección de datos personales" [en línea], *Revista Internacional Online de Derecho de la Comunicación (DERECOM)*, Nueva Época, núm. 13, marzo/mayo, 2013. Dirección URL: http://www.derecom.com/blog/item/download/181_336cdc45b19963d72647d8c2f093d6a7

Garriga Domínguez, Ana, "La protección de datos personales en Internet: problemas actuales" en Álvaro Sánchez Bravo, *Derechos humanos y protección de datos personales en el siglo XXI: homenaje a Cinta Castillo Jiménez,* España, Punto Rojo Libros, 2014, pp. 31-50

Grimalt Servera, Pedro, "La necesaria reconducción del régimen jurídico de la protección de los datos personales desde la perspectiva de los conflictos y

solapamientos con otros derechos y libertades en internet", en Julián Valero Torrijos, *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica,* España, Editorial Thomson Reuters Aranzadi, 2013, pp. 65-87

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), *Guía para titulares de los Datos Personales. Conceptos Generales de la Protección de Datos Personales*, México, Vol. 1, 18 de septiembre, 2017. Dirección URL: http://inicio.inai.org.mx/Guias/Guia%20Titulares-01_PDF.pdf

Iab México, *Estudio de consumo de medios y dispositivos entre internautas mexicanos*, [en línea], México*,* 10ª Edición, julio 2018. Dirección URL: https://www.iabmexico.com/estudios/estudio-de-consumo-de-medios-y-dispositivos-entre-internautas-mexicanos-2019/

Lince Campillo, Rosa María y Fernando Ayala Blanco, *Del lenguaje y su escritura,* México, Universidad Nacional Autónoma de México, 1ª ed., 2017, pp. 133

Ornelas, Lina, "El derecho de las niñas, niños y adolescentes a la protección de sus datos personales: evolución de derechos y su exigencia frente a las redes sociales", en Lina Ornelas y Carlos G. Gregorio (compiladores), *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, Instituto de Investigación para la Justicia (IIJusticia) e Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), México 2011, pp. 73- 127

Ovilla Bueno, Rocío, "La protección de los datos personales en México", México, Porrúa, 2005, pp. 91

Peschard Mariscal, Jacqueline, "Aspectos fundamentales de la protección de datos personales en México", en H. Cámara de Diputados, *Protección de Datos*

Personales. La voz de los actores, México, Tiro Corto Editores, Primera Edición, 2001.

Peschard Mariscal, Jacqueline, "Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos", en Lina Ornelas y G. Gregorio Carlos compiladores, *Protección de datos personales en las Redes Sociales Digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, edición Instituto de Investigación para la Justicia (IIJusticia) e Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), México, 2011. pp. 21-27

Valdivia, Alicia Rubí, "Redes sociales" en Alberto Enrique Nava Garcés, *El derecho en la era digital. Internet, firma electrónica, protección de datos informáticos, comunicaciones, redes sociales, preservación de evidencia,* México, Porrúa, 2013, pp. 67-76

Normatividad mexicana

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), primera edición, diciembre/2017.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), en Marco Normativo de protección de datos personales en posesión de los particulares, Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), primera edición, abril/2014.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Marco Normativo de protección de datos personales en posesión de los particulares, Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), 1ª ed., abril de 2014.

Instrumentos Normativos Internacionales.

Diario Oficial de las Comunidades Europeas, *Carta de los Derechos Fundamentales de la Unión Europea*, Dirección URL: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Resolución de Madrid sobre Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Dirección URL: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

OEA, Informe del Comité Jurídico Interamericano. Privacidad y protección de datos personales, 86º Periodo Ordinario de Sesiones, marzo de 2015. Rio de Janeiro Brasil. Dirección URL: http://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_documentos_referencia_CJI-doc_474-15_rev2.pdf