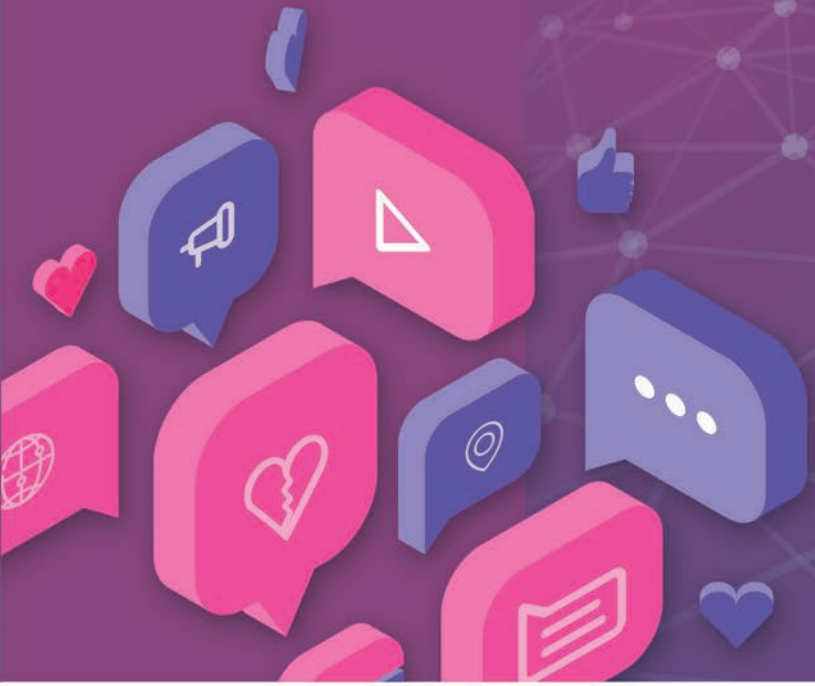
GUÍA ORIENTADORA

"Protección de Datos Personales como herramienta para prevenir la violencia digital"



inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

Comisión de Protección de Datos Personales

GUÍA ORIENTADORA

"Protección de Datos Personales como herramienta para prevenir la violencia digital"

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

Comisión de Protección de Datos Personales

Av. Insurgentes Sur No. 3211, colonia Insurgentes Cuicuilco, alcaldía Coyoacán, Ciudad de México. C.P. 04530.

Primera edición: Julio 2021

Directorio

Blanca Lilia Ibarra Cadena
Comisionada Presidenta del INAI y del SNT

Francisco Javier Acuña Llamas
Comisionado del INAI

Adrián Alcalá Méndez
Comisionado del INAI

Norma Julieta del Río Venegas
Comisionada del INAI

Cinthya Denise Gómez Castañeda
Coordinadora de la Comisión de Protección de Datos Personales del SNT

Oscar Mauricio Guerra Ford
Comisionado del INAI

Rosendoevgueni Monterrey Chepov
Comisionado del INAI

Josefina Román Vergara
Comisionada del INAI

Equipo de Trabajo de la SESNT

Federico Guzmán Tamayo
Secretario Ejecutivo del SNT

José Luis Naya González
Director General de Vinculación, Coordinación y Colaboración con Entidades Federativas

María Elena Vázquez Reyes
Directora de Vinculación y Coordinación con Entidades Federativas

María Guadalupe Manjarrez Segura
Asesora de la SESNT

Paula Angélica Lomelí Cázares
Enlace de la SESNT

Colaboradores

María Antonieta Velásquez Chagoya

José Alfredo Beltrán Estrada

Rebeca Lizette Buenrostro Gutiérrez

Luis González Briseño

Rodrigo Arístides Guerrero García

Norma Julieta del Río Venegas

Laura Lizette Enríquez Rodríguez

Luis Gustavo Parra Noriega

Dora Ivonne Rosales Sotelo

Hugo Alejandro Villar Pinto

Conrado Mendoza Márquez

Josefina Román Vergara

María de los Ángeles Guzmán García

María Elena Guadarrama Conejo

Prólogo

El Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (Sistema Nacional, en adelante) surge como una respuesta del Estado mexicano a la necesidad de implementar políticas públicas que garanticen el ejercicio de los derechos de acceso a la información pública y protección de datos personales, en ocasión de la reforma constitucional en el año 2014.

El Sistema Nacional, en ese sentido, constituye una instancia cuyas estructuras operan a través de procesos democráticos, imparciales y competitivos. Se puede destacar que el Sistema Nacional se encuentra conformado en diez comisiones temáticas, cuatro comisiones regionales y la Coordinación de los Organismos Garantes de las entidades federativas. Estas comisiones, además de fungir como foro de discusiones sobre buenas prácticas, fortalecen el cumplimiento de los objetivos del Sistema Nacional.

Así es como, desde la Comisión de Protección de Datos Personales del Sistema Nacional, se realizan diversos ejercicios promotores del derecho a la protección de datos personales y se generan acciones que orientan a los órganos garantes en la adopción de medidas que garanticen dicho derecho.

Si bien, el funcionamiento de los órganos garantes en las entidades federativas del país, brindan certeza a la ciudadanía sobre la garantía de ejercicio y protección de su derecho fundamental a la protección de datos personales, existe un reto significativo para aumentar la difusión y los conocimientos de todos aquellos beneficios que brinda el derecho a la protección de datos personales frente a cualquier tratamiento de información personal tanto en el contexto privado como en el público.

En los últimos años, las innovaciones tecnológicas han traído consigo diversas prácticas que en el entorno digital implican compartir información personal. La aparición de las tecnologías de la información y comunicación, así como del surgimiento en específico de plataformas digitales, aplicaciones móviles, redes sociales, por mencionar algunas, reorganizan la interacción social (Julio Cabero-Almenara y Julio Ruiz-Palmero, 2017).

Compartir información personal de manera voluntaria o involuntaria en estas plataformas digitales, conlleva la creación de una identidad digital que define quién es cada persona y lleva a la generación de usuarios que, en principio pudieran parecer anónimos, pero en realidad están directamente vinculados a personas en específico. (Teresa González-Ramírez y Angela López-Gracia, 2018).

En los espacios digitales se puede interactuar en múltiples modalidades, ya sea como emisores o receptores de la información, sin embargo, como en cualquier otra interacción social pueden darse actos de violencia que atenten contra las personas, causando un daño psicológico y/o emocional.

La violencia digital es la imposición ilegítima de una voluntad en contra de otra para lograr un fin, ya sea para compartir, manipular o comercializar imágenes, videos o audios de una persona, con contenido íntimo, erótico o sexual, sin su consentimiento libre, pleno y espontáneo; así como la amenaza de difundir esa información para causar un daño (Morales).

Al abordar la violencia digital, se tiene que considerar que existe un tipo de violencia de género digital y que ésta se ejerce en contra de las mujeres, niñas y adolescentes. En el entorno digital existen espacios donde ellas se ven controladas o amenazadas por una tercera persona y tales situaciones, en muchos de los casos, pueden prevenirse si se hace un buen uso de la información personal que se comparte en línea.

La presente guía se propone como una acción formal en la que el Sistema Nacional, toma con seriedad y firmeza disminuir el índice de la violencia digital, pues busca socializar conceptos que toda persona debe conocer al compartir información personal cuando utiliza tecnologías de la información y comunicación.

Cinthya Denise Gómez Castañeda
Coordinadora de la Comisión de Protección de Datos Personales del SNT

Índice

Introducción

El despunte de las Tecnologías de la Información y la Comunicación (TIC) ha provocado grandes oportunidades para el desarrollo y el crecimiento de los países, al impulsar, por ejemplo, las actividades comerciales, la innovación tecnológica y el surgimiento de una gran cantidad de bienes o servicios digitales. A pesar de estas bondades, la revolución digital también ha dado lugar a diversos desafíos para la protección de las libertades y prerrogativas fundamentales de las personas, así como a manifestaciones novedosas de violencia, particularmente contra las mujeres y las niñas por razón de género, lo que restringe su empoderamiento, desarrollo y el pleno disfrute de sus derechos humanos.

Para muestra, en el caso de la República Mexicana, de acuerdo con el Módulo de Ciberacoso 2019, publicado por el Instituto Nacional de Estadística y Geografía, en aquel año, 23.9% de la población de 12 años o más que utilizó internet fue víctima de ciberacoso, lo cual equivale a 17.7 millones de personas, de las cuales 9.4 millones son niñas, adolescentes y mujeres[1].

Bajo este escenario, la Guía orientadora "Protección de datos personales como herramienta para prevenir la violencia digital", promovida por la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia (SNT), representa uno de los desarrollos más importantes de los tiempos recientes, al constituir un documento que permite a las personas identificar qué se consideran datos personales y cuál es la importancia de protegerlos ante el crecimiento exponencial en el uso y el acceso a las TIC, con la finalidad de que puedan adoptar medidas concretas que prevengan, atiendan y erradiquen la violencia digital.

Esta importante herramienta tiene como hilo conductor la protección de datos personales, poniendo en el centro a las personas y a sus derechos, y muestra cómo es que en nuestros tiempos, la dignidad, la libertad de

1 INEGI (2020). "Módulo de Ciberacoso 2019: Principales Resultados", México: INEGI. Consultado el día 18 de junio de 2021. Disponible en: https://www.inegi.org.mx/contenidos/programas/mociba/2019/doc/mociba2019_resultados.pdf

expresión, así como la no injerencia en la vida privada y el acceso a la justicia, quedan en un notorio estado de indefensión, ante una serie de prácticas que, desafortunadamente, se han ido normalizando en el ecosistema digital.

La guía ha tomado en cuenta que la violencia de género contra las mujeres y las niñas en las TIC encuentra, diariamente, nuevas formas para silenciar, excluir o exponer a las mujeres en el espacio digital; ya que, al no contar con el libre acceso a estas tecnologías, se limitan las posibilidades de alcanzar la igualdad entre géneros y, con ello, el ejercicio igualitario de los derechos fundamentales de las niñas y mujeres, incluyendo los de otros grupos en situación de vulnerabilidad.

Actualmente, las TIC están integradas en diversas actividades de nuestra vida cotidiana. Las plataformas digitales están literalmente al alcance de nuestra mano y tienen un papel predominante en la conformación de las identidades y la organización de las interacciones sociales, sobre todo entre la población más joven, pero no se limita exclusivamente a este sector de la población. Por lo anterior, la Guía está prevista para brindar elementos que permitan afrontar el fenómeno de la violencia digital mediante el conocimiento, difusión y sensibilización de las y los titulares sobre el derecho a la privacidad y el ciudado de su información personal.

Los datos personales son particularmente vulnerables cuando se almacenan, comparten y transfieren por las plataformas digitales. Por ello, esta Guía dedica un espacio para explicar y caracterizar en qué consisten los datos personales, entendidos como toda aquella información que pertenece a una persona física identificada o identificable, como lo son: el nombre, la imagen, la edad, el sexo, el domicilio o la nacionalidad, por señalar algunos ejemplos.

Además, la Guía incorpora una reflexión sobre los datos personales de carácter sensible y explica la razón por la que éstos requieren un mayor cuidado y protección, pues al tratarse de información relacionada con la esfera más íntima y privada de una persona –como el estado de salud, las preferencias u orientaciones sexuales, la ideología u opiniones políticas, el origen racial, las creencias religiosas o los datos biométricos–, su indebida utilización puede dar origen a algún tipo de exclusión o discriminación, y generar algún riesgo grave para el titular.

El lector tiene en sus manos una herramienta valiosa en donde encontrará, de manera didáctica y accesible, información relevante sobre diversos tópicos de interés, que van desde el fundamento legal que les permitirá ubicar los elementos de reivindicación, garantía y respeto de sus derechos, hasta la metodología utilizada, la cual destaca, no solo por ser muy acuciosa, sino también colaborativa. Las y los integrantes de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia (SNT) aportaron su conocimiento, su experiencia y su profesionalismo para desarrollar este documento con el objetivo de orientar a las personas, paso a paso, en la comprensión y entendimiento de estos temas.

La Guía ofrece una lista de 14 temas formulados a manera de cuestionamientos, que han sido organizados de lo general a lo particular. Por ello, se parte de un primer bloque donde se reconoce la protección de los datos personales como un derecho fundamental, así como, sus alcances y limitaciones, incluyendo la importancia de adoptar un marco institucional robusto para su resguardo; para seguir entonces con la caracterización de los impactos de las TIC en la garantía de este derecho y la relación que existe entre ambas esferas.

Muy acertadamente se puede identificar otro bloque de preguntas dedicado a concatenar la relación entre privacidad y protección de datos personales, y de ahí a ofrecer una visión que permite comprender en qué consiste la violencia digital y sus distintas manifestaciones; así como, los grupos sociales que son más susceptibles de ser víctimas de ese delito.

Finalmente, hay un conjunto de interrogantes que plantean desde los mecanismos que puede ejercer una persona víctima de violencia digital para proteger su integridad, hasta las instancias a las que debe acudir y las acciones en favor de la protección de datos personales que deben implementarse para combatir esta problemática.

En la mayoría de los casos, la persona que sufre la violencia digital ignora que está siendo víctima de un delito y desconoce las maneras de hacer frente a la situación. Igualmente, puede ignorar que sus derechos están siendo violentados y, por tanto, no tiene acceso a información que le indique los recursos de los que puede disponer o los medios de protección que existen a cada tipo de ataque digital. Por esa razón, tengo la certeza de que esta Guía Orientadora bien puede

contribuir a la protección de las víctimas de este delito, pero también a prevenirlo y combatirlo.

No olvidemos que "lo virtual también es real" y que la violencia ejercida a través de medios electrónicos o del Internet degrada, lastima y afecta la dignidad de las personas y, por tanto, debe erradicarse.

Con la reciente aprobación de la reforma contra el acoso digital, mejor conocida como "Ley Olimpia", sumada a las leyes de acceso a la información y protección de datos personales, junto con la presentación de esta Guía orientadora, avanzamos hacia la configuración y ampliación de los mecanismos que están al alcance de la sociedad, para la protección de las víctimas y la erradicación de esta práctica tan lacerante.

El espacio digital puede, también, incentivar la construcción de nuevas narrativas que contribuyan a fomentar una vida libre de violencia; así como la transformación de normas sociales y culturales, sin discriminación, exclusión y libre de estereotipos de cualquier tipo.

Por todo lo anterior, no queda más que celebrar la materialización de este valioso instrumento en favor de la igualdad sustantiva, el cual pone de manifiesto, nuevamente, la labor de los órganismos garantes y del Sistema Nacional de Transparencia en favor del respeto y la promoción de los derechos de las personas para que con ello, además, favorezcamos los esfuerzos individuales y colectivos para su empoderamiento.

Blanca Lilia Ibarra Cadena
Comisionada Presidenta del INAI

01

El derecho a la protección de datos personales en México

Colaboración de:
María Antonieta Velásquez Chagoya
Comisionada Presidenta del IAIP de Oaxaca

El derecho a la protección de datos personales en México

Para poder hablar sobre datos personales en nuestro país, es importante definir que los datos personales son "Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información"[1] por ejemplo: El nombre, domicilio, huellas digitales, correo electrónico, estado de salud, ideología política, entre otros.

En nuestro país la primer referencia sobre el Derecho a la Protección de los Datos personales se da con la publicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (posteriormente Ley General de Transparencia y Acceso a la Información pública) en el año 2002, pues se contemplan los límites del derecho de acceso a la información estableciendo que los datos personales constituyen información confidencial y requieren del consentimiento de las personas para su difusión, distribución o comercialización.

La reforma del artículo 6to constitucional el año 2007, significó un salto peculiar en lo que refiere el acceso a la información, pues nos da una breve referencia a la privacidad: "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes". Lo que quiere decir, que ya se menciona el derecho a la información y nos remite a una norma secundaria para su desarrollo.

Unos años más adelante en 2009, la misma Consitución reconoce dentro del segundo párrafo del artículo 16 el derecho a la protección de los Datos peronales como un derecho fundamental, reconociendo su autonomía.

1 Artículo 3, Fracción IX de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Un año más tarde en julio de 2010 fue publicada en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y en diciembre de 2016 la Cámara de Diputados aprobó en lo general, el dictamen de la minuta por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, más tarde en enero de 2017 se publicaría en la Primera sección del Diario Oficial de la Federación el decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Al día de hoy la ciudadanía cuenta con Organismos Garantes Locales que protegen sus datos personales contribuyendo a la garantía de sus derechos humanos.

02

¿Qué son los datos personales y cuál es el impacto en el tratamiento?

Colaboración de:
José Alfredo Beltrán Estrada
Comisionado Presidente de la CEAIP de Sinaloa

¿Qué son los datos personales y cuál es el impacto en el tratamiento?

De acuerdo con la legislación mexicana[1], los datos personales son toda aquella información que pertenece a una persona física identificada o identificable, es decir, se refiere a aquella información que nos proporciona una identidad, como lo son, nuestro nombre, imagen, edad, sexo, domicilio, nacionalidad, C.U.R.P (Clave Única de Registro de Población), R.F.C. (Registro Federal de Contribuyentes), estado civil, entre otros.

Además de los ejemplos mencionados, podemos encontrar distintas categorías de datos personales, por ejemplo, los electrónicos, como puede ser el correo electrónico, cuentas y contraseñas, también aquellos académicos, laborales, patrimoniales y biométricos, por mencionar algunos más.

Asimismo, contamos con datos personales que son de carácter sensible, éstos requieren mayor cuidado y protección, pues se considera que al tratarse de información sobre la esfera más íntima de una persona, su indebida utilización puede dar origen a algún tipo de discriminación o conllevar un riesgo grave.

En esta categoría de datos sensibles se encuentra el estado de salud de una persona, ya sea presente o futuro, es decir, el conocer si una persona presenta alguna enfermedad o es sometida a cierto tipo de tratamiento médico, significa adentrarnos a un aspecto de su vida íntima y privada.

Igualmente, conocer sobre las preferencias u orientaciones sexuales, ideología, opiniones políticas, origen racial o creencias religiosas de alguien, podría generar un riesgo significativo al exponerse ante una situación de exclusión o marginación.

En la actualidad, la relevancia que representa el uso de las tecnologías como aplicaciones, herramientas y redes sociales en Internet, así como

1 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y Ley Federal de Protección de Datos Personales en Posesión de Particulares.

su uso cotidiano, nos ha llevado a utilizar nuestros datos personales a través de éstos, incluso a veces hasta de manera excesiva y sin algún tipo de cuidado.

En el entorno digital, es muy común proporcionar nuestros datos personales para realizar diversos tipos de operaciones electrónicas, ya sea para efectuar trámites en línea, compras, transacciones, suscripciones o bien, al realizar publicaciones en redes sociales compartiendo imágenes o diversa información sobre nuestra vida privada.

Al momento de crear una cuenta en alguna plataforma o red social, mínimamente nos solicitan nuestro nombre, apellidos, edad, sexo, nacionalidad, localidad y número telefónico, en la mayoría de los casos.

Es de gran relevancia tomar en cuenta que, al entregar esta información nos hacemos plenamente identificables como personas.

A pesar de ello, olvidamos que al proporcionar nuestros datos personales a través de medios digitales implica, a su vez, un aprovechamiento o tratamiento por parte de empresas o personas, por esta razón es sumamente importante controlar y concientizarnos sobre su uso.

Para ello, debemos interesarnos sobre los términos y condiciones a los que estarán sujetos nuestros datos y leer el aviso de privacidad, ya que en ocasiones las finalidades a las que estarán sometidos no son exactamente para las cuales los proporcionamos.

También, es importante verificar la temporalidad de su uso y si se harán transferencias a terceros, así como el motivo de tal acción.

En el caso de las redes sociales, exponer o sobreexponer nuestra vida privada (tanto nuestra como de familiares y amigos), ideas, opiniones, imágenes, ubicación y relaciones afectivas, nos puede poner en situaciones de riesgo al encontrarse al alcance de otras personas, a veces extraños, pues no solo corremos peligro de sufrir una suplantación de identidad, estafas o robo de datos sino también nos arriesgamos a sufrir violencia digital, de ahí el impacto que representa su uso en el entorno digital.

Incluso, es frecuente encontrarnos con la exposición de datos personales hasta de menores de edad, compartiendo su nombre, imagen y, escuela a la que asisten, invadiendo con ello su privacidad y también exponiéndolos a un peligro latente.

Además, debemos tomar en cuenta que al realizar estas acciones dejamos huella en Internet y todo lo compartido en la red es muy difícil que sea eliminado por completo, a decir verdad, puede resultar imposible.

03

¿Qué es la privacidad como derecho humano y su impacto?

Colaboración de:
Rebeca Lizette Buenrostro Gutiérrez
Comisionada del ITAI de Baja California Sur

¿Qué es la privacidad como derecho humano y su impacto?

En las últimas décadas han sido exponenciales las nuevas e innovadoras formas de comunicarnos, en particular a través de las tecnologías digitales que han jugado un papel preponderante en el cómo y con quién decidimos compartir los aspectos más íntimos de nuestra persona y entorno. Dichas tecnologías de la información y comunicación ofrecen atractivas formas de conectar a las personas entre sí a través de diversos dispositivos y herramientas que no sólo privilegian la rapidez y efectividad de la comunicación, sino que también forman parte sustancial en el desarrollo de la sociedad en diversos ámbitos al facilitar el manejo de información: crearla, transmitirla, enriquecerla y transformarla en conocimiento.

El Instituto Nacional de Estadística y Geografía (INEGI), a través de su Encuesta Nacional Sobre Disponibilidad y Uso de Tecnologías en los Hogares del año 2019, refiere datos significativos que revelan la nueva realidad en la que se vive; donde el 70.1% de la población de seis años o más en México que corresponde a 80.6 millones de personas, son usuarias de Internet. De las principales actividades realizadas por la población con acceso a internet el 90.6% corresponde a las comunicaciones, siendo las redes sociales como el facebook, whatsapp, instagram y youtube las mas significativas.

Como se aprecia, la penetración de las tecnologias de la información y la comunicación procuran áreas de oportunidad en espacios públicos y privados que permiten estar al día y avanzar en los vertiginosos cambios que la actualidad reclama. Sin embargo, a la par de estas bondades, se presenta una cuestionable encrucijada. Por un lado, las oportunidades y ventajas que brindan las tecnologías de la información y de la comunicación a las cuales se accede con facilidad y, por otro lado, la exposición de la intimidad de las personas y sus espacios.

El ser humano siempre ha buscado para sí y los suyos resguardar su intimidad y su ámbito privado. Es decir, reservar espacios que considera exclusivos respecto a los demás miembros del grupo social. En este sentido se puede entender como lo privado según la Real Academia Española,

todo aquello sobre lo que se tiene derecho a proteger de cualquier intromisión. En ese mismo sentido, Moliner (1999) refiere como privado todo aquello que es personal y familiar, no así lo público o profesional, es decir, la separación de los aspectos más propios y reservados para sí, de la esfera pública o de terceros ajenos.

De los primeros y más recurridos antecedentes en el tema de la intimidad y privacidad, se encuentra la publicación del artículo El derecho a la privacidad, de Samuel Warren y Lois Brandeis, en la revista de la asociación de derecho de Harvard, de diciembre de1980. En dicho artículo se expone con acertada precisión la necesidad de regular y proteger por el derecho los aspectos más personales e íntimos de las personas, toda vez que son parte esencial de la dignidad humana. Así pues, se puede apreciar desde la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana de Derechos Humanos, la Convención sobre los Derechos del Niño, la Constitución Política de los Estados Unidos Mexicanos y las resoluciones del Poder Judicial de la Federación, que el derecho a la intimidad a la privacidad son derechos humanos.

Los derechos humanos, afirma Rocatti (1995) son aquellas facultades, libertades y prerrogativas inherentes a la persona humana, que le corresponden a su propia naturaleza, indispensables para asegurar su pleno desarrollo dentro de una sociedad organizada, mismos que deben ser reconocidos y respetados por el orden público o autoridad al ser garantizados por el orden jurídico positivo, por ello el Estado no solo tiene la encomienda de reconocerlos, sino de garantizarlos y salvaguardarlos, puesto que, en palabras de Escalona (2004) todo ordenamiento jurídico, que no reconozca y garantice el pleno ejercicio de los derechos fundamentales –que no los proteja eficazmente- no es un orden justo de convivencia.

Así pues, se reconoce el derecho a la privacidad y a la intimidad como un derecho humano protector, donde el individuo de manera voluntaria constriñe al Estado y a sus congéneres, de interferencias injustificadas en su vida.

04

¿Qué se entiende por protección de datos personales y cuáles son sus alcances?

Colaboración de:
Luis González Briseño
Comisionado Presidente del ICAI de Coahuila

¿Qué se entiende por protección de datos personales y cuáles son sus alcances?

La protección de datos personales se debe entender como el derecho humano a nivel constitucional que tiene toda persona física, independientemente de su origen étnico o nacional, género, edad, discapacidades, condición social, condiciones de salud, religión, opiniones, preferencias sexuales, estado civil, o cualquier otro elemento que pudiera atentar contra su dignidad y/o afectar sus derechos y libertades fundamentales.

Este derecho se encuentra establecido en el artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, que textualmente señala "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."

Actualmente y con el uso de las tecnologías de la información y de la comunicación, podemos encontrar, datos personales en formatos digitales, que sin lugar a dudas también deben de encontrase protegidos independientemente del formato.

Los principios de protección de datos personales son reglas básicas que deben observar los sujetos obligados que tratan datos personales de personas físicas, para garantizar un uso adecuado de la información personal de quienes los proporcionan y es en el artículo 16 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, donde se establece que el responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, principios que se explican en los artículos 17, 18, 19, 22, 23, 25, 26, 29 y 30 de la Ley General en cita.

El principio de licitud, se establece en el artículo 17 y señala que, los datos personales deberán recabarse de manera lícita, de acuerdo a las disposiciones establecidas en la legislación en materia de datos personales. La obtención de datos no puede hacerse a través de métodos engañosos o fraudulentos.

El principio de finalidad, se establece en el artículo 18 y preceptúa que, todo tratamiento de datos personales que efectúe el responsable, deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, o en el caso de empresas privadas, que el tratamiento de datos personales se limite al cumplimiento de las finalidades previstas en el aviso de privacidad.

El principio de lealtad, se establece en el artículo 19 y señala que, el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos. Tendrá que privilegiar la protección de los intereses del titular de los datos personales y la expectativa razonable de privacidad, y velará por el cumplimiento de los principios de protección de datos personales, debiendo adoptar medidas necesarias para su aplicación.

El principio de consentimiento, se norma en el artículo 22 y establece que, todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas en la legislación en la materia.

El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos cuando, habiéndose puesto a su disposición el aviso de privacidad, no manifiesta su oposición. Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo excepciones de ley.

El principio de calidad, se señala en el artículo 23 y preceptúa que, el responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados según los fines para los cuales fueron recabados. Se presume que se cumple con la calidad en

los datos personales, cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.

El principio de proporcionalidad, se explica en el artículo 25 y establece que, el tratamiento de datos personales será el que resulte necesario, adecuado y relevante en relación con las finalidades previstas en el aviso de privacidad.

El principio de información, se norma en el artículo 26 y explica que, el responsable tendrá la obligación de informar a los titulares de los datos, la información que se recabe de ellos y su finalidad; esto, a través del aviso de privacidad, redactado en un lenguaje claro y comprensible, a fin de que aquéllos puedan tomar decisiones informadas al respecto. Asimismo, este principio se refiere a la potestad que otorga la Ley, de conocer previamente las características esenciales del tratamiento a que serán sometidos los datos personales que se proporcionen a un ente privado o empresa.

Finalmente, el principio de responsabilidad, se encuentra en los artículos 29 y 30, los cuales señalan que, el responsable deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él, o por terceros con los que guarde alguna relación jurídica.

05

¿Cuál es la relación entre privacidad y protección de datos personales?

Colaboración de:
Rodrigo Arístides Guerrero García
Comisionado del INFO de la Ciudad de México y Secretario de la Comisión de Datos Personales

¿Cuál es la relación entre privacidad y protección de datos personales?

Este cuestionamiento asume una gran importancia en el contexto actual del advenimiento de las Tecnologías de la Información y la Comunicación y de la emergencia sanitaria global provocada por la pandemia del virus COVID-19. Sin embargo, aunque además de luces, igualmente pueden advertirse sombras en la materia, como la invasión a la privacidad, el ciberacoso o la violencia digital, que se han hecho presentes en el contexto estas importantes renovaciones.

Incluso, desde antes a este acontecimiento que marcó la vida de la humanidad en su conjunto, en México, por ejemplo, al 2019, y con base en el estudio Módulo sobre el Ciberacoso, la población de 12 años y más estimada por la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) era de 101.5 millones de personas.

De ese total, 72.9% utilizó Internet en cualquier dispositivo en los últimos tres meses. De la población usuaria de Internet, 23.9% declaró haber vivido, en los doce meses previos al levantamiento de este estudio, alguna situación de acoso cibernético por las que se indagó, siendo ligeramente mayor para mujeres (24.2%) que para los hombres (23.5%).

Las situaciones experimentadas con mayor frecuencia por parte de la población de mujeres que ha vivido ciberacoso fueron: recibir insinuaciones o propuestas sexuales (40.3%), contacto mediante identidades falsas (35.3%) y recibir mensajes ofensivos(33.9%); mientras que para la población de hombres que han vivido ciberacoso fueron: recibir mensajes ofensivos(33%), contacto mediante identidades falsas (31.6%) y recibir llamadas ofensivas (24.9%).

Como se puede advertir con estas alarmantes cifras, resulta urgente emprender medidas tendientes a la promoción y sensibilización de la población usuaria del internet y de las autoridades en la materia para dar cuenta de la importante necesidad de establecer y potencializar

los entramados normativo e institucional para la protección de la privacidad de los datos personales.

Y es que no puede ignorarse la importante relación entre conceptos como la privacidad y la protección de datos personales. Resulta por demás nítida y clara su intensa interrelación e interdependencia. En ese sentido, valdría la pena dar una revisión a la manera en que se ha definido normativamente a los datos personales, que son toda aquella información que se relaciona con nuestra persona y que nos identifica o nos hace identificables. Nos dan identidad, nos describen y precisan, tales como nuestra edad, domicilio, número telefónico, correo electrónico personal, trayectoria académica, laboral o profesional, patrimonio, número de seguridad social, CURP, entre otros.

Incluso, existen otros que agudizan la relación entre la protección de los datos personales y la privacidad, a saber: los datos personales sensibles, que describen aspectos más delicados, tales como: nuestra forma de pensar, estado de salud, origen étnico y racial, características físicas (ADN, huella digital), ideología y opiniones políticas, las creencias o convicciones religiosas o filosóficas, las preferencias sexuales, entre otros.

Así las cosas, la protección de datos personales a partir de las diversas herramientas normativas e institucionales resulta verdaderamente provechosa. Piénsese por ejemplo en la solicitud de derechos ARCO, con la cual se puede ejercer el control sobre los datos personales y se manifiesta a través del Acceso, la Rectificación, Cancelación y Oposición de dicha información. A través de ella, se puede: i) conocer en todo momento quién dispone de tus datos y para qué están siendo utilizados; ii) solicitar rectificación de tus datos en caso de que resulten incompletos o inexactos; iii) solicitar la cancelación de los mismos por no ajustarse a las disposiciones aplicables; y, iv) oponerse al uso de tus datos si es que los mismos fueron obtenidos sin tu consentimiento. Esta importante herramienta se encuentra regulada en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Es por demás común la problemática en torno a proporcionar datos en sitios de internet o aplicaciones sin consultar los propósitos de recabar dicha información, ni el tratamiento que se les dará. Y es que la experiencia señala que, en Internet, cuando se obtiene un "beneficio gratuito", es muy probable que sus datos se compartan con fines publicitarios; en términos llanos, el usuario o usuaria se convertirá en el "producto".

Finalmente, cabe señalar que por cuanto hace a la regulación de la protección de datos personales existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, enfocada el tratamiento de datos personales por parte de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos,del ámbito federal,estatal y municipal[1].

Asimismo, en el ámbito local, cada entidad federativa del país deberá contar con una ley específica que señale las disposiciones que regularán el tratamiento de datos personales en el sector público de su propio ámbito territorial y que esté armonizada con la Ley General[2].

Respecto del sector privado, existe una sola ley de carácter nacional que regula el tratamiento de datos personales por parte de las personas físicas y morales de carácter privado: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento. Así como diversos materiales normativos, tales como: I) Lineamientos del Aviso de Privacidad; II Criterios Generales para la instrumentación de medidas compensatorias sin la autorización expresa del INAI; III) Lineamientos para el uso de hiperenlaces o hipervínculos en una página de Internet del INAI, para dar a conocer avisos de privacidad a través de medidas compensatorias; iv) los Parámetros de Autorregulación en Materia de Protección de Datos Personales; y, v) las Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante[3].

1 INAI, op. cit., p. 9.

2 Idem.

3 Idem.

06

¿Cuál es el impacto de las Tecnologías de la Información en la protección de los datos personales?

Colaboración de:
Norma Julieta del Río Venegas
Comisionada del INAI

¿Cuál es el impacto de las Tecnologías de la Información en la protección de los datos personales?

El impacto puede ser comprendido de dos formas. La tecnología que por su diseño está programada para tener injerencia sobre la vida privada y por otro lado por las prácticas y usos que hagan las personas de los artefactos. A partir de la evidencia empírica acumulada en los últimos años se pueden considerar dos puntos:

A. El significado de la tecnología parte de sus diseñadores y los conceptos que éstos tengan sobre lo que harán los usuarios. Esto significa que los fabricantes de las nuevas tecnologías integran elementos que condicionan a los usuarios sobre su uso.

En el caso de los datos personales, vale la pena señalar que la mayoría de las tecnologías actuales que se derivan de internet están diseñadas para recordar. Desde casi cualquier lugar con disponibilidad tecnológica y conexión a internet se puede comprar ropa en línea, conocer el pronóstico del tiempo, consultar los estados bancarios, descargar libros, pagar impuestos, comunicarse casi instantáneamente con otras personas, reproducir música, "participar" en actividades políticas, leer el periódico, atender los espacios personales de comunicación, etcétera. Estas prácticas que de alguna forma se vinculan a la vida privada son recordadas por las tecnologías.

Un ejemplo de ello es la red social de Facebook, si bien es gratuita, su uso está condicionado a que las personas sacrifiquen su privacidad. Lo mismo ocurre con las otras dos compañías pilares de la red social: Instagram y WhatsApp. Las prácticas que las personas hacen en estas redes sociales son utilizadas para diseñar nuevos productos, para campañas publicitarias, para mercadeo e incluso con fines políticos.

B. Los seres humanos son capaces de "leer" la tecnología como si se tratara de un texto. En este sentido diversos estudios (Grint y Woolgar, 1997) consideran que las personas son quienes deciden el uso que hacen de la tecnología y no la misma tecnología. Bajo esta condición se deben

considerar factores culturales, políticos y económicos que también pueden definir la forma en la cual las personas usan la tecnología (MacKenzie y Wajcman, 1985).

Las decisiones humanas sobre su privacidad se ven alteradas por la presencia de las tecnologías. Por ejemplo, a diferencia de los adultos, los jóvenes exteriorizan más datos personales, principalmente fotografías en redes sociales (Sabater, 2014). Un estudio del IAB (Interactive Advertising Bureau) realizado en 2017 en varias partes del mundo, detectó que el 80% de los usuarios de redes sociales utilizan estos espacios para publicar sus estados de ánimo, los lugares a los cuales viajaron y comparten fotos o videos de lo que realizan cotidianamente.

Ante lo anterior se puede concluir que la presencia de nuevas tecnologías en la vida diaria de las personas tiene un impacto directo sobre la privacidad. Por un lado, aplicaciones como los navegadores de internet o los servicios de televisión digital como Netflix están codificados para recolectar información sobre las prácticas de los usuarios, y por otro lado, las personas de forma consciente o inconsciente transparentan su privacidad por el simple hecho de que existen medios para hacerlo. Dicha transparencia está determinada en gran medida por la edad y por factores externos, como la cultura, la educación, la religión, etcétera.

07

¿Qué distinción existe en la normatividad de protección de datos personales en el sector público y privado?

Colaboración de:
Laura Lizette Enríquez Rodríguez
Comisionada del INFO de la Ciudad de México

¿Qué distinción existe en la normatividad de protección de datos personales en el sector público y privado?

En México, la protección de datos personales tiene una doble vertiente, pues existe una legislación para instituciones públicas (LGPDPPSO) y otra para particulares (LFPDPPP), es decir, personas físicas o morales del ámbito privado que realicen un tratamiento de datos. Ante esta duplicidad, concurren ciertas diferencias en el tratamiento de datos personales para cada sector, entre las que se destacan:

1. Derecho de portabilidad: Mientras la LGPDPPSO establece la prerrogativa del titular de recibir del responsable una copia de los datos personales objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que permita seguir utilizándolos, la LFPDPPP no contempla dicha prerrogativa.

2. Evaluaciones de Impacto a la protección de datos personales: En la Ley para el sector público, las evaluaciones de impacto se definen como el documento mediante el cual los sujetos obligados que pongan en operación o modifiquen sistemas que impliquen un tratamiento intensivo o relevante de datos personales valoran los impactos reales a efecto de identificar y mitigar posibles riesgos. Para el sector privado se establecen como estudios de impacto sobre la privacidad, previstos como una de las atribuciones que tiene el INAI, los cuales deben solicitarse previo a la puesta en práctica de una nueva modalidad o modificaciones sustanciales de tratamiento de datos personales.

3. Programa Nacional de Protección de Datos Personales: Para la LGPDPPSO este Programa constituye un instrumento rector para la integración y coordinación del SNT, determinando y jerarquizando los objetivos y metas que se deben cumplir en materia de protección de datos personales, la LFPDPPP no lo contempla.

4. Oficial de Protección de Datos Personales: La Ley para el sector público establece que los responsables que lleven a cabo tratamiento de

datos personales relevantes o intensivos, podrán designar un oficial de protección de datos, por otro lado, la Ley del sector privado no contempla dicha figura.

5. Procedimiento de verificación: Tanto en la LGPDPPSO como en la LFPDPPP se contempla el procedimiento de verificación, sin embargo, el primer ordenamiento establece que dicho procedimiento tendrá una duración máxima de 50 días no prorrogables, facultando al INAI para ordenar medidas cautelares. Por otro lado, el segundo ordenamiento contempla un plazo de 180 días prorrogables para la sustanciación de este procedimiento, sin la facultad de imponer medidas cautelares.

6. Auditorías voluntarias: Mientras que la Ley para el sector público establece que los responsables pueden someterse de manera voluntaria a la realización de auditorías por parte del INAI, con el objeto de verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento sus disposiciones, la Ley para el sector privado no la menciona.

7. Casos especiales de tratamiento: La LGPDPPSO regula el ejercicio de derechos ARCO para el caso de personas fallecidas y de menores de edad o personas que se encuentren en estado de interdicción o incapacidad declarada, mientras que la ley para el sector público no contiene preceptos al respecto.

8. Medios de impugnación: Para el sector privado, en tanto un responsable se niegue a atender una solicitud de derechos ARCO, los titulares tienen la opción de presentar una solicitud de protección de datos ante el INAI, y contra las resoluciones del Instituto, los particulares podrán promover el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa. En el sector público, los titulares tienen la opción de promover el recurso de revisión ante el órgano garante, en caso de no estar conformes, la segunda instancia es el recurso de inconformidad ante el INAI o el juicio de amparo ante el Poder Judicial de la Federación, siendo las resoluciones inatacables para los sujetos obligados de la norma.

9. Facultad de atracción: En el sector público, el INAI puede hacer uso de su facultad de atracción para conocer los recursos de revisión que por su interés y trascendencia así lo ameriten, siendo competencia original de los órganos garantes locales. En la LFPDPPP no se contempla la facultad de atracción por ser facultad exclusiva del INAI.

10. Vistas: Para el sector público es posible dar vista del asunto al Órgano de Control Interno, al superior jerárquico o al órgano revisor del sujeto obligado infractor. En la LFPDPPP, solo se establece la facultad del órgano garante de dar vista al propio responsable dentro del procedimiento de una solicitud de protección de datos por la falta de respuesta a una solicitud de derechos ARCO.

11. Medidas de apremio: Mientras que la LGPDPPSO, prevé el establecimiento de medidas de apremio como la amonestación o la multa para asegurar el cumplimiento de las determinaciones del órgano garante, para el sector privado solo se prevé la multa como una sanción a las infracciones en contra de la ley, sin embargo, no se establecen medidas de apremio.

12. Imposición de Sanciones: En el sector privado el procedimiento de imposición de sanciones es efectuado por el INAI, para la Ley General se prevé remitir el asunto a la autoridad competente, quien impondrá o ejecutará directamente al sujeto implicado.

13. Capítulo de delitos: La LFPDPPP contiene en su capítulo XI el establecimiento de un catálogo de Delitos en Materia del Tratamiento Indebido de Datos Personales, a comparación de la LGPDPPSO que no cuenta con uno similar.

08

¿Qué es violencia digital?

Colaboración de:
Luis Gustavo Parra Noriega
Comisionado del INFOEM del Edo. de México

¿Qué es violencia digital?

La problemática de las distintas violencias que aquejan nuestra sociedad, generalmente comienzan dentro de la propia familia, siendo detonantes una variedad de factores que parten de la falta de acceso a la de educación y transitan gradualmente por los insultos, las agresiones y el abuso físico; provocando que los miembros más jóvenes aprendan a interrelacionarse de esta forma en diversos contextos de su vida cotidiana[1].

Es así que, para poder erradicar los distintos tipos de violencia, resulta necesario comprenderlos desde una perspectiva multicausal que concibe a la violencia en general, como un sistema que parte de la interacción comunicativa entre dos o más personas, genera efectos en quienes participan de esta interrelación y trasciende a una realidad colectiva en la que toda la sociedad se encuentra implicada y es responsable[2].

Hoy en día se ha demostrado que el sector poblacional que sufre mayor violencia en su esfera personal es el de las mujeres; los datos que ha aportado la Organización Mundial de la Salud (OMS) y sus Asociados, demuestran que la violencia contra la mujer continúa siendo una problemática generalizada y devastadora, que se empieza a sufrir a edades alarmantemente tempranas. Cerca de 736 millones de mujeres (es decir, una de cada tres) sufren violencia física o sexual infligida por un compañero íntimo o agresiones sexuales perpetradas por otras personas, cifras que se han mantenido estables a lo largo del decenio más reciente[3].

1 José Tovar y Feggy Ostrosky. (2013). Mentes criminales ¿Eligen el mal? Estudios de cómo se genera el juicio moral. México: Manual Moderno.

2 Reynaldo Perrone y Martine Nannini. (2010). Violencia y abusos sexuales en la familia, una visión sistémica de las conductas sociales violentas. Buenos Aires-Barcelona-México: Paidós.

3 Comunicado de Prensa. (09 de marzo de 2021). La violencia contra la mujer es omnipresente y devastadora: la sufren una de cada tres mujeres. Consultado el 06 de mayo de 2021, Organización Mundial de la Salud. Disponible en: https://www.who.int/es/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence

En la actualidad, es imposible desvincular el espacio físico en el que nos desenvolvemos del espacio virtual en el que prolongamos nuestras relaciones sociales con los demás; sin embargo, a pesar de las enormes ventajas, que la Internet y las TIC´s ofrecen a nuestra sociedad, éstas tienden a reproducir las estructuras sociales, más amplias, en las que se manifiestan las diversas formas de violencia contra la mujer, al tiempo que aparecen otras nuevas, propias del entorno digital[4].

El desarrollo exponencial de estas tecnologías ha propiciado la proliferación de conductas que afectan directamente a los usuarios de las mismas, aunque en mayor proporción a las mujeres, representando incluso nuevas amenazas, derivadas de la velocidad con la que la información se difunde en este entorno; la posibilidad de acceder a la información gracias a los motores de búsqueda; la viralidad y la falta de olvido de esta información disponible en la red, representan dificultades adicionales para su eliminación.

Es por esta razón que recientemente se ha avanzado en el desarrollo conceptual de un nuevo tipo de violencia, conocido como violencia digital, la cual es menester definir a continuación:

La violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmite; comercialice, oferte, intercambie o comparta imágenes, audios, o videos reales o simulados de contenido intimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

4 Red Iberoamericana de Protección de Datos (RIPD) del 4 de marzo de 2021. Declaración de la Red Iberoamericana de Protección de Datos (RIPD) contra la Violencia Digital en mujeres y niñas. Consultada el 07 de mayo de 2021. Disponible en: https://www.redipd.org/sites/default/files/2021-03/declaracion-RIPD-contra-violencia-digital.pdf.

Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación.[5]

Este tipo de violencia se perpetra a través de los medios digitales, como redes sociales, correo electrónico o aplicaciones de mensajería móvil, sin embargo, no está desconectada de la violencia que se vive fuera del mundo online. Causa daños a la dignidad, la integridad y/o la seguridad y, tiene impacto en los cuerpos y las vidas de las personas.

5 Gaceta Parlamentaria No. 5770-IV. Palacio Legislativo de San Lázaro, a jueves 29 de abril de 2021, pág. 89. Disponible en: http://gaceta.diputados.gob.mx/PDF/64/2021/abr/20210429-IV.pdf.

09

¿Cuáles son los tipos de violencia que se manifiestan de manera frecuente en el entorno digital?

Colaboración de:
Dora Ivonne Rosales Sotelo
Comisionada Presidenta del IMIPE de Morelos

¿Cuáles son los tipos de violencia que se manifiestan de manera frecuente en el entorno digital?

De acuerdo a las cifras del Censo 2019 elaborado por el Instituto Nacional de Estadística y Geografía (INEGI), en México 70.1 % personas son usuarios de internet; en ese contexto tenemos que, 101.5 millones de la población mayor de 12 años hace uso frecuente de este servicio, empleando el mayor tiempo de conexión para: entretenimiento, buscar información, comunicarse, contenidos audiovisuales, redes sociales y actividades relacionadas a la educación.

Así tenemos que, de la población usuaria del servicio de internet, 38.7% son mujeres y 35.3% hombres; de las cuales el 87.8% se encuentran en un rango de edad de 12 a 17 años; 91.2% de 18 a 24 años, 86.9% de 25 a 34 años; 79.3% de 35 a 44 años; 66.2% de 45 a 54 años y 34.7% de 55 a más; siendo estos los principales grupos.

Es importante partir de este contexto social, debido a que son estos los sectores que se encuentran mayormente expuestos a los actos de violencia digital y los catalogados como delitos cibernéticos. Debemos entonces diferenciar qué acciones son consideradas violencia digital y cuales configuran delitos.

Los delitos cibernéticos, delitos informáticos o delitos hechos mediante computadoras han sido definidos por la Organización de Cooperación y Desarrollo Económico (OCDE) como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos". De igual forma, la ONU reconoce varios tipos de delitos cibernéticos, entre los cuales los más comunes son los relacionados con la identidad.

En nuestro país no existe una regulación específica para los delitos informáticos, si bien se pueden encontrar sanciones para ilícitos llevados a cabo mediante recursos tecnológicos en diversos ordenamientos, siendo el sector financiero el que más ha avanzado en este

aspecto, un hecho que no es de sorprenderse pues en México el delito mediante computadoras que más se lleva a cabo es el fraude, llamado "fraude cibernético".

Por su parte, en la pregunta anterior definimos a la violencia digital como el comportamiento deliberado que puede provocar daños psicológicos o emocionales que refuerzan o incentivan los prejuicios, dañan la reputación y plantean barreras a la participación pública y que son cometidos a través de los medios digitales como redes sociales, correo electrónico, internet, aplicaciones de mensajería móvil, etc.

Tanto la violencia digital como los delitos cibernéticos ocurren a distinta escala dependiendo el grupo social sobre el cual se ejercen; es decir, las mujeres de entre 30 y 40 años no sufren el mismo tipo de violencia que los hombres en el mismo rango de edad o que las mujeres en un rango distinto. Esto se debe a que cada grupo social configura una serie de vulnerabilidades que los vuelve víctimas potenciales.

En el mismo orden de ideas, sería incorrecto encuadrar a la violencia digital en aquella que se comete únicamente por razones de género o la relacionada a temas de índole sexual, pues existe también la violencia política, la discriminación por preferencias religiosas, la suplantación de identidad, el engaño o manipulación contra menores de edad, por mencionar algunas.

Por otra parte, debemos tomar en cuenta las cifras de percepción de violencia que publica el INEGI mediante el censo 2019 donde reporta que 8.3 millones de hombres y 9.4 millones de mujeres ha manifestado ser víctima de alguno de los tipos de violencia digital o delitos, mientras que la información publicada por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública respecto de la Incidencia delictiva del Fuero Común se encuentra la clasificación de delitos digitales; por lo que se refleja un claro vacío en cuanto a delitos que se podrían tipificar respecto a la violencia digital y conocer cuántos de estos son denunciados y más aún cuantos han llegado a una resolución judicial.

La siguiente tabla muestra cuáles son los tipos de violencia o ciberacoso que el INEGI contempla dentro del censo 2019.

CLASE	TIPO	PRINCIPALES GRUPOS VULNERABLES
Criticas por apariencia o clase social.	Violencia	60.7% hombres 73.6% mujeres
Suplantación y/o robo de identidad.	Delito	43.9% mujeres 43.5% hombres
Monitoreo y acecho	Violencia	41.2% hombres 58.7% mujeres
Contacto mediante identificaciones falsas.	Violencia	25.4 hombres 40.7 mujeres
Mensajes ofensivos.	Violencia	47.5 % hombres 40.1 % mujeres
Llamadas ofensivas.	Violencia	33.1 hombres 32.7 mujeres
Publicación de información personal o intima sin consentimiento	Delito	35.6 hombres. 55.1 mujeres
Provocaciones para reaccionar de forma negativa	Violencia	53.9 % hombres 61.8% mujeres.
Insinuaciones o propuestas sexuales	Delito	36.7 % hombres 28.3 % mujeres
Recepción de contenido sexual	Delito	33.6 hombres 26.2 mujeres

Sin embargo podemos detectar otros tipos de violencia o delitos que se pueden cometer a través del Internet.

Discriminación por algún tipo de preferencia	Violencia
Acceso o control no autorizado de los dispositivos de un tercero.	Violencia
Amenazas y agresiones.	Delito
Secuestro	Delito
Extorsión	Delito
Desprestigio o difamación.	Violencia

10

¿Por qué la protección de los datos personales es una herramienta para la prevención de la violencia digital?

Colaboración de:
Hugo Alejandro Villar Pinto
Comisionado Presidente del ITAIPCH de CHIAPAS

¿Por qué la protección de los datos personales es una herramienta para la prevención de la violencia digital?

En la actualidad, hacemos uso excesivo de dispositivos móviles e internet, redes sociales, mensajería instantánea y servicios de geolocalización; así como la publicación de datos personales, fotos y videos; de manera indiscriminada; sin pensar en sus implicaciones; ya que de la misma forma que ha proliferado el uso de estas herramientas tecnológicas, se han incrementado también las conductas de violencia, ciber acoso, humillación, chantaje, amenazas, expresiones ofensivas; lo que demuestra que muchas veces, la internet y sus servicios y aplicaciones, son utilizados para desarrollar estas conductas violentas y se ha convertido en el instrumento más utilizado para estos fines.

Lo anterior es posible debido a la facilidad de acceso a la información que ofrecen los motores de búsqueda y las complicaciones para la eliminación de la información compartida, así como su perduralibilidad en el entorno digital. Si además sumamos a esto el hecho de que las vulneraciones a los datos personales no son percibidas por la ciudadanía como un riesgo cotidiano, el problema se vuele mayúsculo y preocupante; y nos invita a mantenernos alerta.

Es cierto que el proceso de integración tecnológica es inevitable y trae consigo muchos beneficios, pero también supone riesgos potenciales e incertidumbre en el tratamiento que reciben los datos personales de sus titulares.

Cuando realizamos esta integración, debemos informarnos de manera adecuada acerca de la protección de datos personales en el uso de las nuevas tecnologías de la información. Es importante conocer las potenciales situaciones de riesgo en un ámbito como el tecnológico, que se encuentra en constante evolución, para hacernos de las medidas de seguridad adecuadas y gozar de los beneficios de usar las tecnologías de información, sin afectación a nuestra información personal.

Debemos ser sensibles en la protección de nuestros datos personales y ser conscientes de los riesgos y vulneraciones a los que estamos expuestos en el uso de las tecnologías.

Estar atentos a los riesgos, permitirá también que atendamos la recomendaciones preventivas en el uso adecuado de nuestros datos; informarnos de estos riesgos, hace más factible la atención de las recomendaciones preventivas del uso inadecuado de sus datos. Así, la información sobre los riesgos a los que estamos expuestos, junto con las recomendaciones para disminuirlos, debe ser prioritario en la formación transversal de las personas.

Comprendemos entonces que la ley de protección de datos personales resulta de trascendental importancia porque ofrece los instrumentos y herramientas que permiten combatir de manera efectiva las conductas ilícitas en el entorno digital; en un sentido amplio ofrece un marco normativo que expresa la obligatoriedad de atender las demandas de eliminación de contenido violento u ofensivo con urgencia y premura, en atención a los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). Estos elementos son, por supuesto, insoslayables en la lucha contra la violencia digital.

Por ejemplo, la "Ley Olimpia" ha promovido un conjunto de reformas para sancionar penalmente a las personas que divulguen videos, fotografías o cualquier tipo de material multimedia que viole la privacidad de las personas sin su consentimiento; de igual forma, algunas autoridades han realizado iniciativas en las que se busca atender el acoso mediante la difusión de videos y fotografías sin autorización y de manera ilícita en la red.

Si bien es cierto, resulta urgente la realización de ajustes no solo en los algoritmos de búsqueda sino también en los de almacenamiento de la información; los términos y condiciones de los servicios de redes sociales, correos y demás deben revisarse para proteger los datos y minimizar el riesgo de ciber acoso en todas las modalidades expuestas anteriormente; cada persona puede hacer conciencia de los riegos y tomar las medidas necesarias para proteger sus datos personales, evitando compartir en redes sociales información privada o sensible que pueda ser utilizada en su contra con acciones de violencia digital.

11

¿Qué derechos existen para proteger los datos personales?

Colaboración de:
Conrado Mendoza Márquez
Comisionado Presidente del ITAI de Baja California Sur

¿Qué derechos existen para proteger los datos personales?

El derecho a la protección de los datos personales se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos, como un derecho humano fundamental[1]. El derecho a la protección de datos personales incluye a su vez el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales (Derechos ARCO), que para su efectivo ejercicio es necesario solicitarlo ante el responsable que trata los datos personales, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos que deciden sobre el tratamiento de datos personales, es decir quien usa, obtiene, divulga o almacena, a estos. Los Datos personales en mención puede ser cualquier información concerniente a una persona física identificada o identificable, que puede estar expresada en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, por ejemplo: nombre, apellidos, CURP, estado civil, lugar y fecha de nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios, sueldo, entre otros. Es la información que nos describe, nos da identidad, nos caracteriza y diferencia de otros individuos.

De igual manera tenemos los datos personales sensibles: Refieren información que pueda revelar aspectos íntimos de una persona, dar lugar a discriminación o su indebida utilización conlleva un riesgo grave, tal como origen racial o étnico, estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y preferencia sexual.

El Derecho de acceso, rectificación, cancelación u oposición al tratamiento de datos personales, consiste en que toda persona, como titular de sus datos personales o a través de su representante, tiene derecho a acceder a ellos, a rectificarlos, a solicitar su cancelación u oponerse a su tratamiento. A estos derechos se les conoce, en su conjunto como derechos ARCO. Los derechos llamados ARCO son independientes, por lo

1 Artículo 6o, Apartado A, fracción II y artículo 16.

que el ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio del otro. Sin embargo, según el derecho que se pretenda ejercer, se deberá observar lo siguiente:

Derecho de acceso: A través de este derecho puedes solicitar al responsable del tratamiento de datos personales, conocer que información tuya posee, en las bases de datos, sistemas, archivos, registros o expedientes, con que finalidad, como la obtuvo, durante cuanto tiempo la tendrá en su poder, e incluso una copia de esta.

Derecho de rectificación: tienes derecho a solicitar la corrección de tus datos personales que se encuentren en poder de algún responsable, cuando éstos sean: Inexactos, incompletos o no se encuentren actualizados.

Derecho de cancelación: Es el derecho a solicitar que tu información personal sea suprimida o eliminada de los archivos, registros, expedientes o sistemas con los cuales cuente el responsable.

Derecho de oposición: Es tu derecho a oponerte al tratamiento de tus datos personales que se encuentren en posesión de algún responsable, que se abstenga de utilizar información personal para ciertos fines, por ejemplo, la publicación de datos personales en alguna fuente de acceso público, o de requerir que se concluya el uso de estos a fin de evitar un daño o afectación a su persona.

Para hacer valer los derechos ARCO se deberá hacer a través de una solicitud, cuando esta sea dirigida al sector privado, por escrito ante la persona o departamento designado para tal efecto, o en su caso a través del correo electrónico que haya sido proporcionado para ello, cuando la solicitud sea dirigida al sector público, puede presentarse por escrito directamente ante la Unidad de Transparencia del responsable, mediante correo electrónico o a través del portal oficial de la Plataforma Nacional de Transparencia.

12

¿Qué acciones en materia de protección de datos personales, se pueden implementar cuando se ha sido víctima de violencia digital?

Colaboración de:
Josefina Román Vergara
Comisionada del INAI

¿Qué acciones en materia de protección de datos personales, se pueden implementar cuando se ha sido víctima de violencia digital?

El acelerado crecimiento de las tecnologías de la información y la comunicación (TIC´s) ha detonado el fenómeno de la violencia digital, generando un aumento en las vulneraciones a la intimidad, integridad, seguridad y derechos humanos de todas las personas, exponiendo la seguridad de los datos personales de quienes han sido víctimas de este tipo de violencia.

De acuerdo con la Universidad Nacional Autónoma de México[1], la sociedad mexicana hace un uso intensivo de redes sociales, siendo WhatsApp, YouTube, Twitter, Instagram y Facebook, las 5 redes más usadas; por lo cual es indispensable que todas las personas contemos – en principio - con una adecuada educación digital, para proteger nuestros datos personales en la red y, así, disminuir la vulneración de éstos en las TIC´s.

Al respecto, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha difundido diversas guías y recomendaciones para los titulares para facilitar su seguridad en el entorno digital[2]. Lo anterior, como actos preventivos, que buscan ser una herramienta para que las personas cuenten con conocimiento sobre cómo proteger sus datos personales y, entonces, reducir el riesgo de sufrir violencia digital.

1 Según el estudio "Radiografía sobre la difusión de fake news in México". Disponible en: https://www.dgcs.unam.mx/boletin/bdboletin/2020_318.html
Fecha de consulta 6 de mayo del 2021.

2 Todas las guías se encuentran a disposición del público en general en la siguiente dirección electrónica: https://home.inai.org.mx/?page_id=3402

Sin embargo, ante el aumento de casos de violencia digital entre hombres y mujeres, en cuanto a los aspectos reactivos, la Red Iberoamericana de Protección de Datos Personales ha sostenido que sería deseable que las redes sociales digitales cuenten con canales para que las víctimas puedan solicitar la cancelación de sus datos personales, de carácter urgente. Y, efectivamente, en la actualidad las redes sociales han facilitado el ejercicio de los derechos de cancelación y de oposición, frente a las compañías de la internet, para poner término a la difusión de las informaciones personales en la internet.

Así, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, posibilita a las personas el ejercicio de derechos de Acceso, Rectificación, Cancelación y Oposición de Datos Personales, ante el indebido tratamiento de datos personales en las redes sociales y los motores de búsqueda en la internet.

Y además, el INAI tiene la potestad de tramitar el procedimiento de protección de derechos, como una instancia que procederá cuando el responsable no otorgue respuesta, o se niegue a efectuar modificaciones o correcciones a los datos personales. Asimismo, al INAI le corresponde investigar, por oficio o denuncia, el indebido tratamiento de los datos personales vinculados con la violencia digital, cuando éste, se asocie a la falta de cumplimiento a los principios y deberes previstos en la Ley de la materia y, en su caso, imponer sanciones.

No obstante, es importante señalar que no está facultado para investigar cualquiera de los delitos que se configuren por violencia digital, pues la persecución de este tipo de delito corresponde a la autoridad penal. El pasado 29 de abril del año 2021, la Cámara de Diputados aprobó el paquete de reformas de la llamada "Ley Olimpia", para tipificar como delito la violencia digital, e incluirla como un tipo más de violencia en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia; asimismo, en la Ciudad de México, ya se cuenta con el paquete de reformas legislativas conocida como "Ley Ingrid"[3], las cuales tienen por objeto evitar la exposición de las personas víctimas de violencia en las redes sociales y los medios de comunicación para proteger la intimidad, dignidad y datos personales de las víctimas y la de sus familiares, y combatir con estas reformas la violencia mediática de género y su normalización;

3 http://ordenjuridico.gob.mx/violenciagenero/LEY%20INGRID.pdf

sancionando a las personas y servidores públicos que se involucren en este tipo de conductas.

Finalmente, vale enfatizar que si la víctima de violencia digital tiene conocimiento del tratamiento indebido de sus datos personales, o del responsable del sector público a nivel estatal, ha hecho un mal uso de sus datos personales, puede acudir a los órganos garantes locales, a presentar su denuncia, por las presuntas violaciones a la normatividad que regula el derecho a la protección de datos personales.

Los órganos garantes del Sistema Nacional de Transparencia, asumen y reconocen el compromiso con la erradicación de la violencia digital dentro de la normativa de protección de datos personales, a fin de garantizar los mayores estándares de atención y, con ello, brindar certeza jurídica a las víctimas de violencia.

13

¿Qué derechos en materia de protección de datos personales tiene una víctima de violencia digital respecto del resguardo de su identidad y protección de datos personales?

Colaboración de:
María de los Ángeles Guzmán García
Comisionada de la COTAI de Nuevo León

¿Qué derechos en materia de protección de datos personales tiene una víctima de violencia digital respecto del resguardo de su identidad y protección de datos personales?

Las tecnologías de la información y de la comunicación (TIC) han revolucionado la forma en que la sociedad se comunica y la velocidad con la que se transfieren datos, entre ellos imágenes de las personas. Las TIC, al ser correctamente utilizadas, porporcionan infinitas ventajas a las actividades cotidianas. Sin embargo, el mal uso de ellas, representa riesgos que pueden impactar gravemente la vida y los derechos humanos de quien los padece. Estas consecuencias afectan a las víctimas en su patrimonio, integridad personal y psiquíca, honor, imagen, autoestima, privacidad personal y familiar, identidad, dignidad, libre desarrollo de la personalidad, autonomía, entre otras.

Por una parte, la difusión de imágenes íntimas de una persona (Ley Olimpia), o aquellas producto del escenario de un delito o hallazgo en un procedimiento penal (Ley Ingrid), pueden conducir al suicido. El derecho humano a la protección de datos personales es un derecho personalísimo, que se extingue con la muerte del titular. En el caso de una víctima que pierde la vida, se afectan derechos humanos de quienes integran la familia, no así de quien murió.

Particularmente las mujeres, niñas y adolescentes se han visto gravemente afectadas por la violencia digital producida a través de las TIC, así como por la falta de controles legales, sociales, medidas de seguridad y un mejor sistema de justicia, que faciliten la persecución del comportamiento criminal en línea. Por esta razón, se aprobaron una serie de reformas a diversos ordenamientos en diferentes estados de la República, por ejemplo, el Código Penal del Distrito Federal, la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México y la Ley Orgánica de la Procuraduría General de Justicia del Distrito Federal.

A estas reformas se les denominó, "Ley Olimpia" y "Ley Ingrid" [1]; la Ley Ingrid, es una reforma en materia penal, que busca evitar la exposición de las víctimas de delitos ante los medios para proteger tanto su intimidad y dignidad, como la de sus familiares[2]. Y tiene como objetivos: 1) Tipificar de forma autónoma las conductas que realicen las personas servidoras públicas que de manera indebida revelen o difundan, imágenes, videos o grabaciones; así como archivos o información de la carpeta de investigación; 2) Fortalecer la protección de los derechos de las víctimas; y 3) Combatir la violencia mediática de género y su normalización, sancionando a las personas servidoras públicas que realicen dichas conductas.

El enfoque de la Ley se basa en la intervención de la autoridad competente en la responsabilidad de salvaguardar la identidad y dignidad, así como la protección de los datos personales de las víctimas de violencia digital. Para erradicar este tipo de violencia es necesario sancionar, de manera ejemplar, a quienes la ejercen. Sin embargo, el problema es que las autoridades no cuentan con conocimientos técnicos en la materia, ni protocolos para atender, trabajar, orientar, asesorar y juzgar con perspectiva de género.

---

1 Congreso de la Ciudad de México (2019). "Ley Olimpia" Iniciativa con proyecto de decreto por el que se reforma el nombre del Capítulo III "Acoso sexual", del Título Quinto, del Libro Segundo parte especial, y se adiciona un artículo 179 Bis al Código Penal para el Distrito Federal, y se adiciona una fracción VI al artículo 7 de la Ley de acceso a las mujeres a una vida libre de violencia de la Ciudad de México https://congresocdmx.gob.mx/archivos/parlamentarios/IN_215_10_12_09_2019.pdf (Consultada el 20 de mayo de 2021). Congreso de la Ciudad de México (2020). "Ley Ingrid" Iniciativa con proyecto de Decreto que adiciona un artículo 293 quater, al Código Penal para el Distrito Federal. https://consulta.congresocdmx.gob.mx/consulta/webroot/img/files/iniciativa/IN_295_16_18022020.pdf (Consultada el 20 de mayo de 2021). Esta última, surge a raíz de la difusión indebida en redes sociales y medios de comunicación de las imágenes de un feminicidio ocurrido en la Ciudad de México el 9 de febrero de 2020. La divulgación masiva del cuerpo de Ingrid conmocionó a la sociedad que indignada exigió parar la filtración del expediente de la Fiscalía.

2 A la fecha, luego de siete años de activismo, la Ley Olimpia ha sido aprobada en 29 estados de la República; mientras que la Ley Ingrid, a un año de los hechos que la originaron, en la Ciudad de México, Oaxaca y Colima http://ordenjuridico.gob.mx/violenciagenero/LEY%20INGRID.pdf (Consultada el 22 de mayo de 2021).

14

¿Qué medidas de carácter preventivo en materia de protección de datos personales, pueden ayudar a prevenir la violencia digital?

Colaboración de:
María Elena Guadarrama Conejo
Comisionada del INFOQRO de Querétaro

¿Qué medidas de carácter preventivo en materia de protección de datos personales, pueden ayudar a prevenir la violencia digital?

Según el Instituto Nacional de Estadística y Geografía (INEGI), la violencia digital presente en personas de 12 a 59 años de edad, en un 40.3% se genera sobre las mujeres de 12 años y más, mientras que el 33% de los hombres víctima de ciberacoso recibió mensajes ofensivos.

El INEGI, ha detectado especialmente algunos tipos de ciberacoso, mediante el Módulo sobre el Ciberacoso (MOCIBA) 2019, y lo define como "un acto intencionado, ya sea por parte de un individuo o un grupo, teniendo como fin el dañar o molestar a una persona mediante el uso de tecnologías de información y comunicación, en específico el Internet".

En virtud de ello, se enlistan algunas recomendaciones generales para prevenir situaciones de riesgo:

1. Leer las condiciones de uso al utilizar un servicio digital, para conocer la manera en que pueden utilizar tus datos y los derechos que tienen sobre tu información.

2. Evitar caer en discursos de odio o replicarlos.

3. Cerrar/apagar los equipos, ya que terceras personas pueden utilizar la cámara de los dispositivos para realizar capturas sin tu consentimiento.

4. Crear contraseñas seguras en los dispositivos y no compartirlas.

5. Rechazar la opción de conexión automática que almacena nombre de usuario y contraseña.

6. Evitar dar información personal, como correos electrónicos o números de teléfono a desconocidos.

7. Desactivar el bluetooth y geolocalización cuando no se esté usando.

8. Instalar y actualizar antivirus o firewalls.

9. Utilizar redes seguras, evitar redes de libre acceso y nunca hacer transacciones desde éstas.

10. Revisar estados de cuenta a detalle.

11. Cerrar la sesión cada que se firma en digital, y borrar la memoria cache.

12. Realizar transacciones verificando que se utilice el protocolo de seguridad https.

13. Considerar establecer controles parentales, ya que ha aumentado el número de casos de violencia digital en contra de menores de edad.

14. Evitar enviar contenido íntimo por medio de internet, instalar antivirus certificados en los dispositivos móviles y/o computador y actualizarlos para evitar hackeos.

15. Configurar las opciones de privacidad de las redes sociales, procurando dejar poca información visible para personas desconocidas; no seguir sus cuentas ni aceptarlos en las redes sociales.

16. Denuncia las páginas o perfiles para informar abusos. Guarda los mensajes o la información inadecuada para presentarlos como prueba al momento de realizar la denuncia.

17. Ejercer sus derechos ARCO cuando proceda.

La prevención en el ámbito del uso de la tecnología se convierte en un elemento fundamental para evitar la violencia digital. "La violencia desde donde venga, debe prevenirse por múltiples razones: cuidar la salud y calidad de vida en todo momento y prevenir la tendencia hacia la perpetuación de las situaciones violentas". (Cyberbullying: entre la prevención y la sensibilización).

Como personas hay que evitar caer en la tentación de compartir información delicada, con la cuál incluso publicarla, podríamos incurrir en alguno de los delitos establecidos en los Códigos Penales de los Estados.

La normativa de protección de datos personales, es una vía administrativa que contribuye a proteger la seguridad y derechos de la víctima, para evitar que a la conmoción producida (por el daño físico, psíquico, familiar social o económico) y experimentada por actuaciones reprobables de violencia, se añada una segunda victimización derivada de un inadecuado tratamiento de su información personal en la ejecución de los procesos que la administración destina a la atención y tutela de su situación[3].

Al respecto, uno de los protocolos que se debiesen seguir, es que la Institución a través de su personal ofrezca, a las víctimas o a sus familiares, información suficiente y adecuada relacionada con los datos que se recabarán. En otras palabras, cumplir con la presentación del aviso de privacidad. Idealmente, la autoridad debe de explicar su contenido, señalando para qué finalidad se van a recoger los datos personales. Además, garantizarles que estos serán resguardados bajo la máxima confidencialidad, añadiendo la información sobre quién es la dependencia o la persona responsable de que se utilicen correctamente (tratamiento) y cómo se podrán ejercer los derechos ARCO.

Definitivamente, las víctimas de violencia digital, tienen en todo momento el derecho a la protección de su imagen, respeto, intimidad, dignidad y honor; tienen derecho al debido tratamiento de sus datos personales y que los servidores públicos quienes se involucran en dicho tratamiento, actúen apegados a los principios de ética profesional y defensa de las víctimas.

3 El derecho a la protección de datos personales se ejerce ante una autoridad local o federal que posee información personal y ante la cual se desea promover los derechos ARCO. En caso de inconformidad con la respuesta, se deberá de recurrir, en la vía administrativa, ante el organo garante local o nacional, según sea el caso. Estos últimos protegen dos derechos humanos, el acceso a la información y el de protección de datos personales. El INAI es el órgano garante nacional. Además de esta vía, se podrían ejercer derechos similares, aunque no iguales, por la vía judicial en materia civil y penal.

Referencias

Aumenta la violencia, https://lucesdelsiglo.com/2021/03/09/aumenta-la-violencia-digital-cdmx/

Cerviño, Saavedra, J. y otros (2006). Experiencias de relación en la escuela. Prevenir la violencia contra las mujeres. N° 19. Serie de Cuadernos de Educación no sexista, Madrid: Instituto de la Mujer.

Contreras, Sergio. () Facebook no olvida. Revista Etcétera. Consultado el 5 de mayo de 2021. Recuperado de https://www.etcetera.com.mx/revista/facebook-no-olvida/

Del Río Jiménez, M. (2008). "Creando Redes en coeducación: maletas para la igualdad". Caleidoscopio, revista digital de contenidos educativos, 1, pp. 152-158.

Derechos digitales, https://internetesnuestra.mx/post/180565103773/violencia-digital-un-sistema-que-promueve-la

Escalona, G. (2004). La Naturaleza de los Derechos Humanos. Presente, Pasado y Futuro de los Derechos Humanos. México: CNDH/UNED.

Grint, K. y Woolgar, S. (1997). The machine at work. Cambridge: Polity.

https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543

Instituto Nacional de Estadística y Geografía INEGI | Módulo sobre el Ciberacoso. (2019).Recuperado de: https://www.inegi.org.mx/contenidos/programas/mociba/2019/doc/mociba2019_resultados.pdf

Julio Cabero-Almenara y Julio Ruiz-Palmero. (2017). Las Tecnologías de la Información y Comunicación para la inclusión: reformulando la brecha digital. 10-07-2017, de International Journal of Educational Research and Innovation (IJERI) Sitio web: https://idus.us.es/bitstream/handle/11441/66918/2665-8692-1-PB.pdf?sequence=1&isAllowed=y

Los jóvenes y la vulnerabilidad en la era digital, https://quimica.unam.mx/las-jovenes-el-sector-mas-vulnerable-para-sufrir-violencia-digital/#:~:text=%E2%80%9CSon%20conductas%2C%20sobre%20todo%20de,%C3%ADntimo%20sin%20consentimiento%E2%80%9D%2C%20apunt%C3%B3.

Luchadoras de México, https://luchadoras.mx/13-formas-violencia-linea-las-mujeres/

Mackenzie, D. y Wajcman, J. (1985). The Social Shaping of Technology. Buckingham: Open University Press.

Medina, Diana (2020). Cyberbullying: entre la prevención y la sensibilización. Recuperado de: https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/14381/15543

Módulo sobre Ciberacoso (MOCIBA) 2019, https://www.inegi.org.mx/programas/mociba/2019/

Moliner, M. (1999). Diccionario de uso del español, Madrid, Gredos.

Morales Brand, José Luis Eloy, ¿Qué es la violencia digital?, Universidad, Autónoma de Aguascalientes, https://www.uaa.mx/portal/gaceta_uaa/que-es-la-violencia-digital/

Olivé, L. (2004). Interculturalismo y justicia social. México DF: UNAM. Pantallas amigas. (13 de enero de 2012). Pantallas amigas. Obtenido de Pantallas amigas: https://www.pantallasamigas.net/una-encuesta-internacional-revela-el-alcance-mundial-del-problema-del-ciberbullying T

Real Academia Española, Diccionario de la lengua española , Madrid, Espasa, 2001.

Rocatti, M. (1995). Los derechos humanos y la experiencia del ombudsman en México. México: CDHEM.

Sabater, C. (2014). La vida privad en la sociedad digital. La exposición pública de los jóvenes en internet. Aposta, número 61, pp.1-32.

Téllez Carvajal E. (2017) Reflexiones en torno a la "Ciudadanía Digital" Vol. 7, No. 13, 2017. P-ISSN 2395. Revista Doxa. Méx. UNAM GLOBAL. (18 de 01 de 2018). México, cuarto lugar a nivel mundial en uso de redes sociales. Excélsior, pág. 21.

Teresa González-Ramírez y Angela López-Gracia (2018). La identidad digital de los adolescentes: usos y riesgos de las Tecnologías de la Información y la Comunicación. 8 diciembre 2018, de Revista Latinoamericana de Tecnología Educativa Sitio web: http://dehesa.unex.es/bitstream/10662/8761/1/1695-288X_17_2_73.pdf

Urrutia, A. (12 de Julio de 2016). México, primer lugar en "sexting" en América Latina. La Jornada.

Violencia digital, http://eds.a.ebscohost.com.pbidi.unam.mx:8080/eds/pdfviewer/pdfviewer?vid=6&sid=7c8ae5d1-eb6a-401e-954e-003a29a-776d8%40sessionmgr4008

Warren, S. y Brandeis, L. (1890). The Rigth to Privacy. Harvard Law Review.

Guía Orientadora "Protección de Datos Personales como herramienta para prevenir la violencia digital"

Se terminó de editar en el mes de julio de 2021

Edición a cargo de la Secretaría Ejecutiva del Sistema Nacional de Transparencia (SNT), Dirección General de Vinculación , Coordinación y Colaboración con Entidades Federativas.