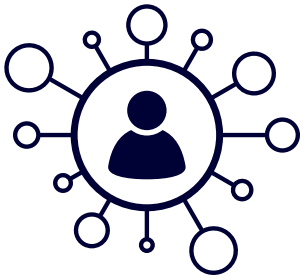

Los riesgos y desafíos de la identidad digital

Xitlali Gómez Terán

Comisionada Propietaria del Instituto Morelense de Información Pública y Estadística

Resumen

La incursión de la sociedad en el ámbito digital se ha traducido en grandes ventajas como el hecho de tener la posibilidad de interactuar con personas de todo el mundo mediante el uso de plataformas digitales con diversos propósitos, no obstante, para tener acceso a ellas, deben registrar sus datos personales; en el presente artículo se reflexiona en torno a los riesgos y desafíos que enfrenta la sociedad para proteger su identidad y evitar ser víctima de algún delito.

PALABRAS CLAVES:
Identidad, Redes sociales, Ciberseguridad

Introducción

El 65% de la población en el mundo es usuaria de internet, por tanto, podríamos señalar que se encuentran de alguna forma, interconectados e interactúan en redes sociales, las cuales tienen como requisito, el registro de datos personales, lo que implica un grave riesgo de que dicha información sea accesible con el efecto de hacer un mal uso y con frecuencia, ser personas sujetas de algún delito.

En el presente artículo se desarrolla una reflexión sobre cuáles son los riesgos a los que nos enfrentamos en esta aldea global, en la que se interactúa de manera creciente y que coloca a las personas en una situación de riesgo, más aún a aquellos grupos en situación de desventaja por la discriminación de que son sujetas.

Por lo anterior, el objetivo es realizar un análisis sobre los riesgos a los que nos enfrentamos como sociedad globalizada e interconectada, al registrar nuestros datos en las diversas plataformas digitales, identificar los más frecuentes y presentar algunas propuestas para proteger los datos personales y contrarrestarlos.

De esta manera, en el primer apartado se presenta un marco conceptual y jurídico sobre el tema, enseguida se exponen los principales riesgos para proteger la identidad digital de las personas, con énfasis en aquellos grupos en desventaja como son los adolescentes y niños, así como las mujeres y las personas con discapacidad, entre otras; finalmente se presentan una serie de reflexiones a manera de conclusión.

Marco conceptual y jurídico

Marco conceptual

Es importante contar con un marco conceptual que permita conocer el contenido de cada uno de los términos a los que se hará referencia en el presente artículo, los cuales se retoman de la Ley General de Protección de Datos Personales en posesión de sujetos obligados.

Datos personales: 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; (Cámara de diputados, 2017, p. 3)

Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual; (Cámara de diputados, 2017, p. 3)

Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales; (Cámara de diputados, 2017, p. 4)

Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades: a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados; b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Revisar la configuración de segu-

ridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales; (Cámara de diputados, 2017, p.5)

Marco jurídico

Se cuenta con un marco jurídico robusto a partir de los siguientes preceptos:

Constitución Política de los Estados Unidos Mexicanos[1]:

> *Art. 6. El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.*

Entre las normas reglamentarias[2] de esta disposición de carácter constitucional se identifican las siguientes:

Ley Federal de Telecomunicaciones y Radiodifusión[3]:

> *Artículo 145. Los concesionarios y autorizados que presten el servicio de acceso a Internet deberán sujetarse a los lineamientos de carácter general que al efecto expida el Instituto conforme a lo siguiente:*
>
> *I. Libre elección. Los usuarios de los servicios de acceso a Internet podrán acceder a cualquier contenido, aplicación o servicio ofrecido por los concesionarios o por los autorizados a comercializar, dentro del marco legal aplicable, sin limitar, degradar, restringir o discriminar el acceso a los mismos. No podrán limitar el derecho de los usuarios del servicio de acceso a Internet a incorporar o utilizar cualquier clase de instrumentos, dispositivos o aparatos que se conecten a su red, siempre y cuando éstos se encuentren homologados;*
>
> *II. No discriminación. Los concesionarios y los autorizados a comercializar que presten el servicio de acceso a Internet se abstendrán de obstruir, interferir, inspeccionar, filtrar o discriminar contenidos, aplicaciones o servicio;*
>
> *III. Privacidad. Deberán preservar la privacidad de los usuarios y la seguridad de la red;*
>
> *IV. Transparencia e información. Deberán publicar en su página de Internet la información relativa a las características del servicio ofrecido, incluyendo las políticas de gestión de tráfico y administración de red autorizada por el Instituto, velocidad, calidad, la naturaleza y garantía del servicio;*
>
> *V. Gestión de tráfico.[4] Los concesionarios y autorizados podrán tomar las medidas o acciones necesarias para la gestión de tráfico y administración de red conforme a las políticas autorizadas por el Instituto, a fin de garantizar la*

[1] Cámara de Diputados, (2024) Constitución Política de los Estados Unidos Mexicanos, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

[2] Existe un análisis realizado por la Cámara de diputados denominado REGULACIÓN DE LAS REDES SOCIALES: ELEMENTOS PARA SU ANÁLISIS. Disponible en: https://www.diputados.gob.mx/sedia/sia/spi/SAPI-ASS-01-22.pdf

[3] Cámara de Diputados, (2021) Ley Federal de Telecomunicaciones y Radiodifusión, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

[4] El tráfico se define de acuerdo con la Ley en comento como: Datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que circulan por una red de telecomunicaciones; (art. 3, fracc. LXIX).

calidad o la velocidad de servicio contratada por el usuario, siempre que ello no constituya una práctica contraria a la sana competencia y libre concurrencia; […]

Artículo 146. Los concesionarios y los autorizados deberán prestar el servicio de acceso a Internet respetando la capacidad, velocidad y calidad contratada por el usuario, con independencia del contenido, origen, destino, terminal o aplicación, así como de los servicios que se provean a través de Internet, en cumplimiento de lo señalado en el artículo anterior.

Por su parte, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[5] establece:

Artículo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Resulta aplicable lo previsto en el artículo 17 del mismo ordenamiento al señalar:

Artículo 17.- El aviso de privacidad debe ponerse a disposición de los titulares a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología, de la siguiente manera:

I. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

II. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

[5] Cámara de Diputados, (2017) Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Descripción de los posibles riesgos asociados con la identidad digital

Con los avances tecnológicos que, sin duda alguna, representaron una serie de beneficios para la sociedad, también se acompañaron de diversos riesgos, entre ellos, la ciberseguridad personal (Escobar, 2024), la violencia digital, la suplantación o robo de identidad entre algunos de ellos.

El Reporte Global Digital 2023 de Meltwater and We are social, indica que hay una población total de 8,010 millones de personas, de las cuales 5,160 millones son usuarias de internet, lo que representa 65% de la población (Mendoza, 2023, párrafo 5)[6]; de manera que es innegable que existe una interacción de las personas en el ámbito digital y por ende, con la posibilidad de interactuar mediante diversas plataformas, entre ellas, las redes sociales, de hecho se reconoce que el 60 % de las personas son usuarias activas en redes sociales.

Por su parte, el INEGI (2022) indicó que en México, de acuerdo a los resultados de la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2021, la población de 12 y más años usuaria de internet fue de 104.2 millones de personas, y que casi ocho de cada diez personas, entre mayo y septiembre de 2021, utilizó internet en cualquier dispositivo.

En el mismo sentido señaló que las personas usuarias de internet en México[7] víctimas de ciberacoso[8] se incrementó de 21 % a 21.7 % en 2021 con una mayor prevalencia en el caso de las mujeres (22.8 %) que en los hombres (20.6 %) identificando que la expresión más frecuente fue el de contacto mediante identidades falsas (INEGI, 2022), no obstante de que para el año 2023 este instituto indicó que se identificó que la población usuaria de internet que fue víctima de ciberacoso disminuyó, de 21.7 % en 2021, a 20.8 % en 2022, lo cierto es que resulta latente el riesgo para las personas de ser vulnerables a este tipo de violencia[9]. (INEGI, 2023)[10]

El INEGI realiza una medición mediante el Módulo sobre Ciberacoso (MOCIBA), el cual explora diversas expresiones como:

i. Recibir mensajes ofensivos, con insultos o burlas;

ii. Recibir llamadas ofensivas, con insultos o burlas;

iii. Ser criticado(a) por su apariencia (forma de vestir, tono de piel, peso, estatura, etc.) o clase social;

iv. Que una persona se hiciera pasar por usted para enviar información falsa, insultar o agredir a otras personas;

v. Ser contactado(a) por medio de nombres falsos para molestarle o dañarle;

vi. Ser vigilado en sus sitios o cuentas en internet para causarle molestia o daño;

vii. Ser provocado en línea para que reaccione de forma negativa;

viii. Recibir insinuaciones o propuestas de tipo sexual que le molestaran;

ix. Recibió fotos o videos de contenido sexual que le molestaron;

x. Publicar o vender imágenes o videos de contenido sexual reales o simulados, de usted sin su consentimiento;

---

[6] Mendoza, Jonathan, (22 de agosto de 2023), Privacidad vs. tecnología: la falsa elección, en El Economista, disponible en: https://www.eleconomista.com.mx/opinion/Privacidad-vs.-tecnologia-la-falsa-eleccion-20230822-0060.html

[7] Se considera como población usuaria a las personas de 12 años y más que utilizaron internet en cualquier dispositivo electrónico en los últimos tres meses, en cada caso. (INEGI,

[8] (…) se refiere a la situación en la que alguien se expone, de manera repetida y prolongada, a acciones negativas por parte de una o varias personas que buscan hacer daño o causar molestias. Los medios que utilizan son electrónicos, como el teléfono celular e internet. INEGI, 2022, p. 1

[9] INEGI, 2022, Comunicado de Prensa Núm. 364/22, 13 DE JULIO DE 2022. Disponible en: www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf

[10] INEGI, 2023, Comunicado de Prensa Núm. 404/23, 13 de Julio de 2023, Módulo Sobre Ciberacoso 2022. Disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf

xi. Publicar información personal, fotos o videos para dañarlo(a);

xii. Amenazar con publicar información personal, audios o video para extorsionar; y

xiii. Otra situación que lo(a) haya afectado. (INEGI, 2022, p. 1)

Para 2022, el INEGI dio a conocer que la población de 12 años y más fue de 105.8 millones de personas, de ellas, 8 de cada diez, entre marzo y agosto de 2022, utilizó internet en cualquier dispositivo, es decir, 84.1 millones de personas: 44.0 correspondió a mujeres y 40.1 millones a hombres. (INEGI, 2023, p.1)

En cuanto al ciberacoso más frecuente que experimentaron tanto hombres como mujeres fue el contacto mediante identidades falsas y la mayor prevalencia se registró en los estados de Tlaxcala, Yucatán y Tabasco, con una mayor prevalencia en el caso de las mujeres (44.0 en mujeres y 40.1 millones, en hombres). (INEGI, 2023, p.1)

El INEGI (2023) indicó que, en el año 2022 el 20 % de hombres y 29 % de mujeres de entre 12 y 19 años de edad y 23.7 % de los hombres y 29.3 % de las mujeres de 20 a 29 años, que utilizaron internet, fueron víctimas de ciberacoso en los últimos 12 meses; es decir, 4 de cada 100 hombres y 6 de cada diez mujeres jóvenes sufrieron ciberacoso en 2022. (INEGI, 2023)

Entre las conductas de ciberacoso que se reportaron en los últimos 12 meses, se identificó que el 36.0 % de las mujeres y 39.0 % de los hombres experimentaron contacto mediante identidades falsas, en tanto que el 34.8 % de las mujeres experimentó insinuaciones o propuestas sexuales y 33.6 % recibió contenido sexual. Para los hombres, estos porcentajes fueron 15.1 y 18.5 %, respectivamente. (INEGI, 2023)

En cuanto a las redes sociales mediante las que se ejerce el ciberacoso es importante destacar que se observa una diferenciación por sexo, de manera que la red social por medio de la que se registró un mayor porcentaje de ciberacoso fue Facebook, 49.3 % para el caso de las mujeres y 38 % en hombres, seguido de WhatsApp con un 40 % en hombres y 36 % en mujeres; en cuanto a las llamadas telefónicas, 33 % en hombres y 24 % en mujeres y por messenger fueron víctimas de ciberacoso el 16.4 % de hombres en contraparte, el 29 % de mujeres. (INEGI, 2023)

Las expresiones del ciberacoso más utilizadas es publicar información personal, fotos o videos en Facebook, con 57.6 %, seguido de WhatsApp, con 34.1 %. Y el enojo es una de las consecuencias que experimentan las víctimas. (INEGI, 2023)

Las consecuencias que pueden derivarse de este tipo de violencia dependen en gran medida de las características de la persona afectada, pero en términos generales, la violencia digital puede traducirse en conductas de violencia en el mundo real como violencia física, sexual, que incluso puede derivar en la muerte de la persona. Asimismo, entre las afectaciones en la salud de las víctimas es frecuente que presenten conductas de autolesionarse que pueden llevar incluso al suicidio. Este tipo de violencia en el ciberespacio puede conducir a las personas adultas a perder su empleo, afectación a su reputación personal y profesional y la cancelación de su proyecto en la esfera pública (UNFPA, 2022, párrafo 4)[11].

Toda persona que interactúa en el ámbito digital puede ser víctima de violencia en el ciberespacio, no obstante, ésta se puede recrudecer cuando pertenecen a grupos históricamente discriminados como mujeres, personas LGBTTTIQ+, de color, con alguna discapacidad, juventudes e infancias entre otras. De ahí que este tipo de conductas provengan de comportamientos de misoginia, racismo y homofobia, en general, de actos de discriminación por algún rasgo, como la edad o el sector poblacional al que pertenece una persona o grupo.

[11] UNFPA, 2021, Documento orientativo para informar sobre la violencia digital: Guía práctica de referencia para periodistas y medios de comunicación, Disponible en: https://www.unfpa.org/es/resources/Documento-orientativo-para-informar-sobre-violencia-digital

Especial relevancia merece la atención que se debe prestar a la niñez y las juventudes que participan en el mundo digital, quienes tienen una mayor exposición porque pasan más tiempo conectados en la red de internet, desconocen los medios para protegerse y las secuelas de la violencia digital puede generar graves daños y limitar su pleno desarrollo. Al respecto, en la Observación general número 25 (2021) relativa a los derechos de los niños en relación con el entorno digital, entre otros aspectos de trascendencia, se hace referencia a que dicho ámbito está en constante evolución, y abarca las tecnologías de la información y las comunicaciones, incluidas las redes, los contenidos, los servicios y las aplicaciones digitales, los servicios, los dispositivos y entornos conectados, la realidad virtual y aumentada, la inteligencia artificial, la robótica, los sistemas automatizados, los algoritmos y el análisis de datos, entre otros. En este documento se señala que es justo ese entorno digital, que reviste una creciente importancia para casi todos los aspectos de la vida de la niñez.

Al respecto, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha puesto énfasis sobre la especial atención que reviste la protección de las infancias, en virtud de los prolongados periodos de tiempo que navegan por la red de internet y en las redes sociales, que requieren del registro de sus datos personales. En nuestro país se estima que el 10 % de los 88.6 millones de internautas, son menores de entre 6 y 11 años de edad y 13. 6 % cuentan entre 12 y 17 años, de acuerdo a datos del 18º Estudio sobre los Hábitos de los Usuarios de Internet en México, de la Asociación de Internet MX. (INAI, 2023, p.2)[12]

En España se ha reportado que entre los riesgos a los que se enfrentan las infancias al utilizar las redes sociales son entre otras: pedofilia, ciberbullyng o acoso escolar, adicciones digitales (juegos online, apuestas, redes sociales), sexting, sextorsión, contactos peligrosos en redes sociales, grooming,[13] contenido inadecuado para niños y niñas, publicar datos privados de la familia, compras online sin permiso y fraude online y Ransmware o secuestro de dispositivos. (Gaptain, s/f)[14]

Recomendaciones para proteger la identidad digital y mantener la privacidad en línea

El INAI ha emitido instrumentos de ayuda para evitar la vulneración de los derechos de las personas que tienen acceso a internet y utilizan redes sociales, entre ellas, la Guía para prevenir el robo de identidad, las Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital, la Guía para la configuración en redes sociales, la Guía de supervisión parental y el Test: ¿Cómo te proteges en redes sociales? [15], que pueden ser de gran utilidad para proteger a las personas en el ciberespacio.

En este sentido, al tratarse de los menores de edad el INAI brinda las siguientes recomendaciones con el fin de protegerles:

1. *Supervisión parental. Involucrarse en el uso que hacen niñas, niños y adolescentes de las redes sociales como una medida de prevención, con respeto a la privacidad y al interés superior del menor.*

2. *El poder de la red. Informar a personas menores de edad que la información que se publica en internet se propaga velozmente; por ello, es importante establecer configuraciones de privacidad a fin de controlar quien tiene acceso a su información personal.*

[12] INAI, 2023, menores, más expuestos a ser víctimas de ciberacoso; INAI emite recomendaciones para evitarlo. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-081-23.pdf

[13] Internet da la opción a pederastas de hacerse pasar por menores para acercarse a ellos.

[14] Gaptain, s/f, Prevención de riesgos digitales, Disponible en: https://gaptain.com/riesgos-de-internet-y-moviles/

[15] Herramientas que pueden ser consultadas en el sitio web: https://home.inai.org.mx/?page_id=3402

3. *Límites claros. La interacción, a través de redes sociales, debe ser con personas conocidas; evitando aceptar como amigos a quienes no se conoce en persona.*

4. *Cuidar su privacidad. Fomentar el uso de cuentas privadas en redes sociales. Es importante que no compartan información sensible (imágenes íntimas o comprometedoras, contraseñas, geolocalización, mensajes que pudieran perjudicarles, etcétera).*

5. *Proteger su dispositivo electrónico. Fijar una contraseña segura o método de desbloqueo de la pantalla, y establecer configuraciones seguras para aumentar la protección de los menores.*

6. *Educación digital. Localizar y analizar recursos existentes como películas, notas informativas, casos reales en los medios de comunicación, que ayuden a orientarles sobre los riesgos que corren en internet, cuando no se toman medidas de seguridad.*

7. *Cambios de conducta. Vigilar cualquier cambio de conducta repentino que no sea común en las y los menores. Muchas de las veces estos cambios pueden estar relacionados en la etapa de la adolescencia; sin embargo, hay que estar alerta de conductas inusuales.*

8. *Consentimiento. Consentir el uso de redes sociales y el acceso a plataformas de internet, de acuerdo con su edad y nivel de madurez.*

9. *Confianza. Generar espacios que fortalezcan la comunicación entre menores y adultos para facilitar, en su caso, la detección de algún problema. (INAI, 2023,p.2)*[16]

Por su parte, el INEGI (2023) reportó que en los últimos tres meses de 2022, el 74.1 % de las personas que utilizaron internet en cualquier dispositivo, reportó haber adoptado alguna medida de seguridad para proteger su computadora, tableta electrónica, teléfono celular o cuentas de internet, el 95.6 % reportó crear o poner contraseñas (claves, huella digital, patrón, etcétera) como medida principal y 27.4 % señaló instalar o actualizar programas antivirus, cortafuegos o antiespías. (INEGI, 2023, p. 18)

No obstante, es menester fortalecer las medidas con el fin de prevenir los riesgos del robo de identidad o el mal uso de las cuentas de redes sociales, así como el ciberacoso, por lo que se exponen algunas de ellas:

1. Actualizar el software regularmente: mantener actualizados nuestros equipos y aplicaciones es uno de los factores que fortalece la seguridad e impide el ataque de nuevos virus informáticos.

2. Tener precaución al navegar en internet: revisar los enlaces antes de hacer clic sobre ellos, en especial con las noticias falsas (las famosas “fake news”) que se han convertido en un método frecuente para llevar a cabo ciberataques.

3. Navegar solo en sitios seguros: evitar facilitar datos personales hasta verificar el nivel de seguridad del portal. La indicación “https” antes de la URL indica que se trata de una conexión segura, protegida por una tecnología encriptada.

4. Es importante estar al día en medidas de seguridad cibernética. Los expertos en ciberseguridad descubren nuevos métodos para proteger los datos personales de los internautas.

[16] INAI, 2023, menores, más expuestos a ser víctimas de ciberacoso; INAI emite recomendaciones para evitarlo. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-081-23.pdf

5. Utilizar conexiones WI-FI protegidas de cifrado WPA: evitar redes inalámbricas como las que ofrecen lugares públicos, ya que puede dejar sus datos expuestos. (Retomado del Prestador de servicios de certificación Uanataca)[17].

6. En caso de enfrentar acoso digital mediante redes sociales se cuenta con diversos recursos, por ejemplo en Facebook[18] disponen de recursos que pueden ayudar, Twitter[19], así como en Instragam[20] y Tik Tok[21]. (UNICEF, s/f).[22]

Reflexiones finales

Dado que es inevitable el uso de las nuevas tecnologías, el acceso a internet y la utilización de diversas plataformas, entre ellas, las redes sociales, por parte de las personas, es imprescindible el conocimiento de los riesgos implícitos, por lo que se deben implementar mayores medidas de seguridad a las y los internautas y con especial énfasis en las personas que pertenecen a un grupo en desventaja dado que presentan una mayor vulnerabilidad.

En este artículo se expusieron algunos de los riesgos que conlleva el uso de la red de internet y las redes sociales por parte de la población, así como algunas de las expresiones del ciberacoso y sus consecuencias así como algunas recomendaciones que son de utilidad para proteger a las personas usuarias de los servicios de internet y de plataformas digitales, la expectativa es que se contribuya a difundir los riesgos pero también las buenas prácticas para incursionar en el ciberespacio de manera segura.

[17] UANATACA, (s/f) seis consejos para protegerla. Disponible en: https://web.uanataca.com/es/blog/transformacion-digital/proteger-identidad-digital

[18] https://www.facebook.com/safety/bullying

[19] https://help.twitter.com/en

[20] https://about.instagram.com/es-la/safety y https://about.instagram.com/es-la/community/anti-bullying

[21] https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-video y https://www.tiktok.com/safety/es-es/bullying-prevention/

[22] UNICEF, (s/f), Ciberacoso: Qué es y cómo detenerlo. Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Fuentes de consulta

Cámara de Diputados, (2017) Ley Federal de Protección de Datos Personales en Posesión de los Particulares, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Cámara de Diputados, (2021) Constitución Política de los Estados Unidos Mexicanos, disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_280521.pdf

Cámara de Diputados, (2021) Ley Federal de Telecomunicaciones y Radiodifusión, disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf

Gaptain, s/f, Prevención de riesgos digitales, Disponible en: https://gaptain.com/riesgos-de-internet-y-moviles/

INAI, 2023, menores, más expuestos a ser víctimas de ciberacoso; INAI emite recomendaciones para evitarlo. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-081-23.pdf

Escobar Ruiz, Dylan, (2024) Amenazas a la ciberseguridad personal: el desafío que enfrenta el mundo este 2024, INFOBAE, Disponible en:

INAI, 2023, menores, más expuestos a ser víctimas de ciberacoso; INAI emite recomendaciones para evitarlo. Disponible en: https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-081-23.pdf

INEGI, 2022, Comunicado de Prensa Núm. 364/22, 13 DE JULIO DE 2022. Disponible en: www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/mociba/MOCIBA2021.pdf

INEGI, 2023, Comunicado de Prensa Núm. 404/23, 13 de Julio de 2023, Módulo Sobre Ciberacoso 2022. Disponible en: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf

Mendoza, Jonathan, (22 de agosto de 2023), Privacidad vs. tecnología: la falsa elección, en El Economista, disponible en: https://www.eleconomista.com.mx/opinion/Privacidad-vs.-tecnologia-la-falsa-eleccion-20230822-0060.html

UANATACA, (s/f) seis consejos para protegerla. Disponible en: https://web.uanataca.com/es/blog/transformacion-digital/proteger-identidad-digital

UNFPA, 2021, Documento orientativo para informar sobre la violencia digital: Guía práctica de referencia para periodistas y medios de comunicación, Disponible en: https://www.unfpa.org/es/resources/Documento-orientativo-para-informar-sobre-violencia-digital

UNICEF, (s/f), Ciberacoso: Qué es y cómo detenerlo. Disponible en: https://www.unicef.org/es/end-violence/ciberacoso-que-es-y-como-detenerlo

Xitlali
Gómez Terán

Maestra en Derecho Electoral por la Escuela Judicial Electoral del TEPJF; Especialista en Derecho Constitucional por la División de Estudios de Posgrado de la Facultad de Derecho de la UNAM, titulada con mención honorífica y Licenciada en Derecho por la Facultad de Derecho de la Universidad Autónoma de Guerrero, titulada con mención honorífica. Actualmente Comisionada Propietaria del Instituto Morelense de Información Pública y Estadística.