VOCES Y SABERES

Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

Medidas de protección del usuario de Internet

Denisse Damaris Torres[1]

Resumen

Las ventajas del uso de Internet son innumerables, sobre todo en el rubro de comunicación, y han propiciado el incremento en las interacciones en la red; pero también han potencializado los riesgos de ser víctima de diversas conductas delictivas sancionables, principalmente, de índole patrimonial, pornografía y delincuencia organizada; no obstante, en muchos casos son conductas prevenibles. La educación e información de los usuarios de Internet son los medios más efectivos para prevenir daños causados por *malware* (afectaciones al sistema informático mediante determinados programas), *phishing* (estafas), *pharming* (robo de datos personales) y ciberacoso, ya que si implementamos configuraciones de seguridad y privacidad adecuadas al uso de nuestros dispositivos, lograremos disminuir las amenazas. Desde luego, además de instalar antivirus y actualizaciones que añaden candados de seguridad y logran la adecuada transmisión de información, aunados al comportamiento de civilidad de cada uno de los usuarios, en el que se eviten señalamientos, discriminación y ofensas, con el fin de mantener todas las navegaciones de forma segura.

[1]Denisse Damaris Torres licenciada en Derecho por la FES Aragón. Colaboradora en el Programa de Maestría en Derecho de la División de Estudios Posgrado y docente en la Licenciatura de Derecho del SUA de esta Facultad.
Apoyo académico con experiencia en plataformas académicas de la DUACyD, en el desarrollo de materiales didáctico pedagógicos para las aulas virtuales y construcción de aulas virtuales.
Ponente en diferentes diplomados y curso de Actualización y Formación Docente de la DGAPA.

ABSTRACT

The advantages of Internet use are innumerable, especially in terms of communication, and have led to an increase in online interactions, which in turn has increased the risks of being a victim of various punishable criminal behaviors, mainly of a patrimonial nature, pornography and organized crime, however, in many cases these behaviors are preventable. The information and education of Internet users are the most effective means for the prevention of damages caused by Malware, Phishing, Pharming and cyberbullying, managing to reduce the threats if we implement security and privacy settings appropriate to the use we make in our devices in addition to the installation of antivirus and updates that add security locks and achieve the proper transmission of information, coupled with the correct humanized behavior of each of the users without discrimination, signaling and offenses to keep all browsing as a safe place.

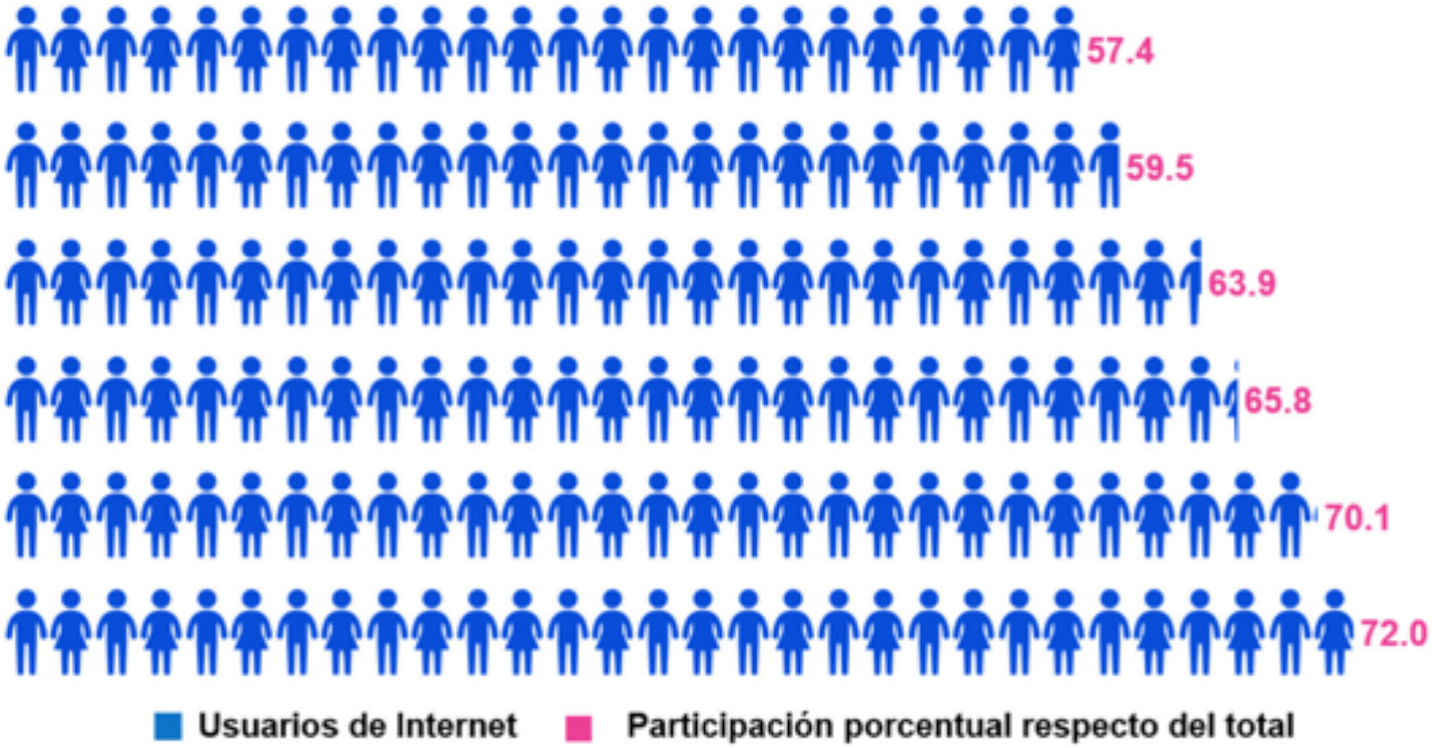
Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

Introducción

La contingencia sanitaria causada por el virus SARS-CoV-2 ha cambiado todas las interacciones humanas, obligándonos a buscar una manera de mantener distanciamiento social y, a la par, realizar diversas actividades cotidianas. Esto ha revolucionado la forma en que compramos, vendemos, trabajamos, o nos entretenemos, educamos, divertimos y numerosas actividades más. Tales acciones incrementaron la navegación en Internet y nos convirtieron en usuarios de algunas herramientas esenciales en la transmisión y recepción de datos en general.

Según datos del Banco Mundial, en los últimos cinco años hubo un incremento de usuarios de Internet, ya que de 40.90% de la población mundial que lo empleaba en 2015 se llegó a 56.72% en 2019. Tan solo en México, hasta 2020, había 72% de usuarios, lo que se traduce en 84.1 millones de personas que interaccionan de alguna forma en la red y en cada una de estas actividades van dejando una huella digital (Instituto Nacional de Estadística y Geografía [INEGI], 2021) (Figura 1).

Figura 1. *Población usuaria de Internet en México, 2015-2020.*



Fuente: Tomado de Instituto Nacional de Estadística y Geografía (2021, 22 de junio). En México hay 84.1 millones de usuarios de internet y 88.2 millones de usuarios de teléfonos celulares: ENDUTIH 2020 [Comunicado de prensa]. (p. 4).

El incremento de usuarios y actividades en Internet también conlleva el aumento de riesgos y formas en las que podemos ser engañados, suplantados, estafados, o de sufrir robo de propiedad intelectual, por ello es esencial hablar de ciberseguridad y ciudadanía digital.

Con la reforma al artículo 1803 del Código Civil para el Distrito Federal. Se expidió la Ley de Ciudadanía Digital de la Ciudad de México (vLex, 2020) que define, en su numeral segundo, fracción novena:

> … **IX. Ciudadanía Digital:** Condición que identifica a una persona a través de medios digitales para realizar trámites, servicios, así como actos jurídicos y administrativos a cargo de la Administración Pública y las Alcaldías de la Ciudad de México (Ley de Ciudadanía Digital de la Ciudad de México, 2020).

Por lo tanto, el ciudadano digital es la persona capaz de ejercer sus derechos y obligaciones en el uso de las tecnologías de la información y la comunicación (TIC).[2]

[2]En México es poco el avance en las cuestiones sobre la ciberseguridad, la Secretaría de Seguridad Ciudadana cuenta con una Unidad de Policía Cibernética que mantiene un monitoreo de 24 horas en redes y fuentes abiertas de Internet; ofrece pláticas informativas para la prevención de los delitos cibernéticos e informa acerca de las alertas creadas, principalmente, a partir de las denuncias de la población. Entre las acciones más importantes se encuentra el reconocimiento y prevención de conductas delictivas. La víctima de un delito cibernético puede contactar con esta unidad a través del correo electrónico policia.cibernetica@ssc.cdmx o del teléfono 52425100 ext. 5086. Gobierno de la Ciudad de México. (s.f.). Secretaría de Seguridad Ciudadana. https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica. https://www.ssc.cdmx.gob.mx/

Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

Riesgo en línea

La intención de los delitos cibernéticos es afectar al usuario, principalmente en su patrimonio, aunque existen otros perjuicios a los bienes jurídicos tutelados (vida, seguridad, libertad, integridad, libertad sexual, etc.), como los casos de pornografía y delincuencia organizada. Por lo general, los infractores acceden de forma ilegal a la información personal contenida en los dispositivos electrónicos de los usuarios, o con programas que descargan, y entre los riesgos más comunes se enlistan los siguientes:

1. *Software malicioso y virus*. Son programas diseñados para dañar el dispositivo y robar información del usuario, o ambos, y operan de distintas formas: ya sea monitoreando la actividad en Internet, guardando y enviando datos, ocupando espacio de almacenamiento, eliminando o dañando archivos, o mostrando publicidad; se puede instalar con autorización del usuario, o sin ella, según el tipo de *malware*.

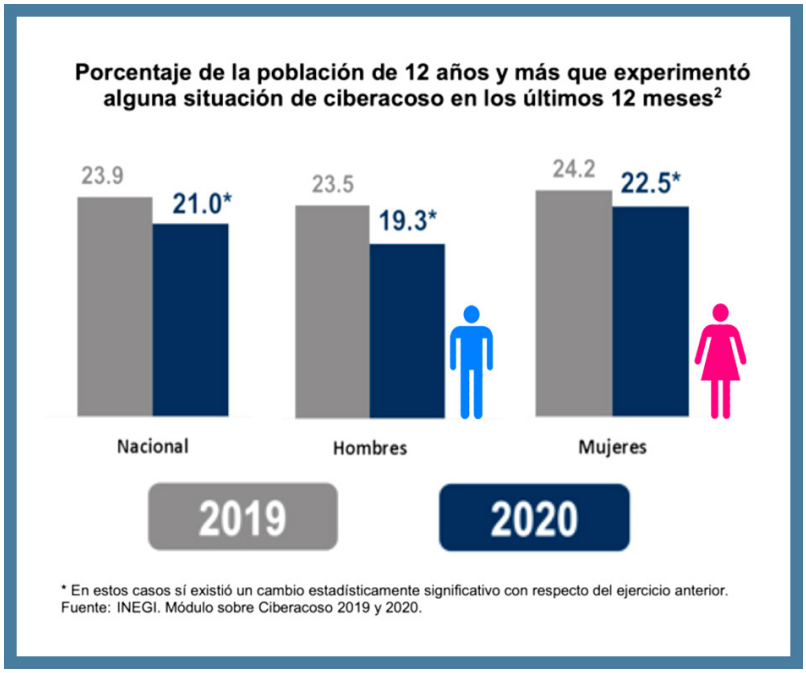
2. *Phishing y Pharming*. Es la "Estafa que tiene como objetivo obtener a través de internet datos privados de los usuarios, especialmente para acceder a sus cuentas o datos bancarios" (*Oxford Dictionary, 2022*). Se realiza mediante la recepción de un correo electrónico o mensajería instantánea con aparente remitente de persona "conocida" o "institución reconocida", con los que se engaña a los usuarios para que proporcionen sus datos personales.

3. *Ciberacoso*. Se refiere al comportamiento que busca perjudicar de forma reiterada a una persona o un grupo, mediante mensajes o contenidos, expresados en burlas, humillación y discriminación. Este hostigamiento repercute de forma física, mental o emocional en la víctima y le genera vergüenza, temor, terror, frustración, tristeza y depresión.

En México, en 2020, el INEGI implementó un módulo para denunciar el ciberacoso y generar información estadística sobre este ciberdelito, del que se observan como principales resultados los siguientes:

> De acuerdo con los resultados de la Encuesta Nacional sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH) 2020, en México, 75% de la población de 12 años y más utilizó Internet en cualquier dispositivo en el periodo comprendido entre julio y noviembre de 2020.
>
> De la población usuaria de Internet referida en el párrafo anterior, 21% declaró haber vivido, entre octubre de 2019 y noviembre de 2020, alguna situación de acoso cibernético por las que se indagó, siendo mayor para mujeres (22.5%) que para los hombres (19.3%). Los adolescentes y jóvenes son los más expuestos: 23.3% de los hombres de 20 a 29 años y 29.2% de las mujeres de 12 a 19 años, señalaron haber vivido algún tipo de ciberacoso.
>
> ...De la población usuaria de internet, 21% vivió alguna situación de acoso cibernético en los últimos 12 meses. Esto equivale a 16.1 millones de personas de 12 años y más usuarios de internet a través de cualquier dispositivo durante 2020 en México, 9 millones de mujeres y 7.1 millones de hombres. (Figura 2).

Figura 2. *Comparativo estadístico del periodo 2019-2022, de población de 12 en delante que padeció ciberacoso.*



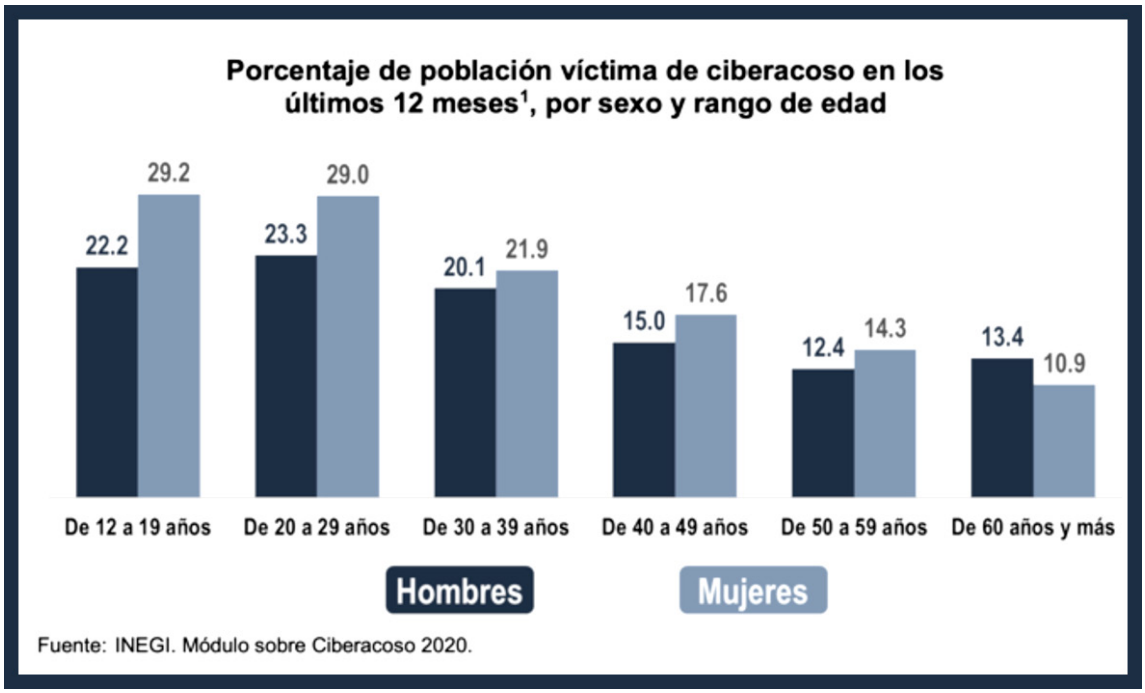
Fuente: Tomado del Instituto Nacional de Estadística y Geografía (2021, 5 de julio). Módulo sobre ciberacoso 2020. [Comunicado de prensa]. (p. 7).

DATA LEAK
SECURITY BREAC
EXPLOIT FOUNDED
VIRUS DETECTE

Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

También se muestra que los rangos de edad de las víctimas influyen: quienes más sufren por estas conductas delictivas son las mujeres de entre 12 y 19 años (Figura 3).

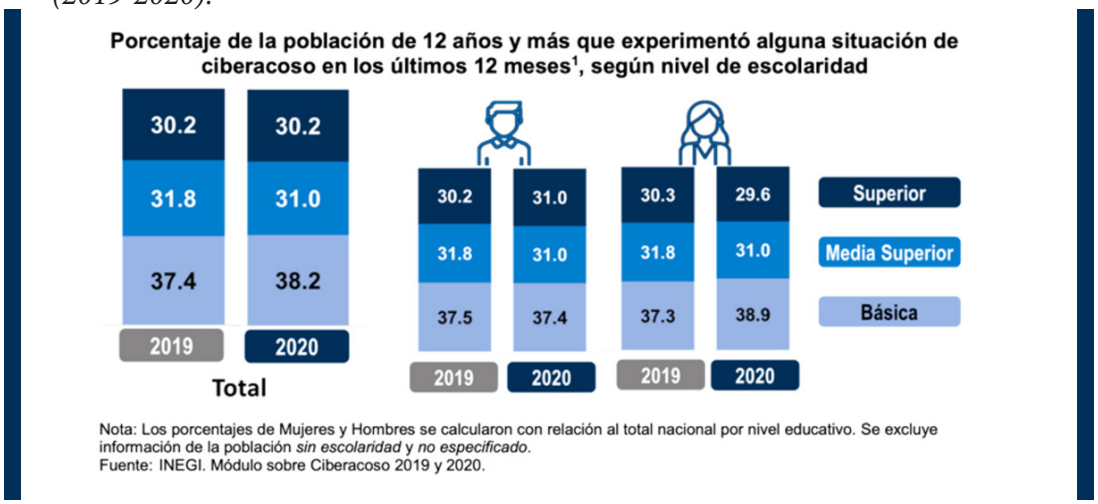
Figura 3. *Comparativo de población víctima de ciberacoso por edades (2020).*



Fuente: Tomado del Instituto Nacional de Estadística y Geografía (2021, 5 de julio). Módulo sobre ciberacoso 2020. [Comunicado de prensa]. (p. 7).

En cuanto al nivel de estudios de las víctimas, se observa que quienes tienen el nivel básico de estudios sufre mayor ciberacoso, pero es importante apuntar que a menor edad, mayor vulnerabilidad, por lo que no es sorpresa que en niveles de estudios más elevados se reduzca esta conducta (Figura 4).

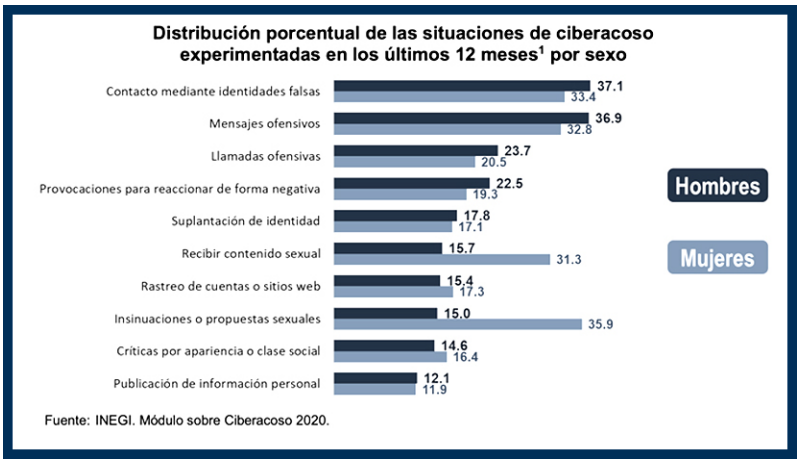
Figura 4. *Comparativo de población víctima de ciberacoso por nivel escolar (2019-2020).*



Fuente: Tomado del Instituto Nacional de Estadística y Geografía (2021, 5 de julio). *Módulo sobre ciberacoso 2020.* [Comunicado de prensa]. (p. 12).

De las situaciones reportadas que experimentan las víctimas, el acoso de índole sexual es de las conductas más repetitivas, donde 35.9% de las mujeres recibieron insinuaciones o propuestas sexuales, y 31.3%, también de mujeres, informó que recibió contenido sexual sin solicitarlo (Figura 5).

Figura 5. *Comparativo de situaciones de ciberacoso por género (2020).*



Fuente: Tomado del Instituto Nacional de Estadística y Geografía (2021, 5 de julio). *Módulo sobre ciberacoso 2020.* [Comunicado de prensa]. (p. 14).

Mitigación del riesgo

La principal medida de seguridad disponible es la actualización de los equipos, ya que los creadores y proveedores de *software* se encuentran en constante estudio de los programas dañinos y añaden innovaciones a los candados de seguridad y posibles fallas para proteger nuestros equipos.

Asimismo, el uso adecuado de antivirus también puede protegernos y alertarnos sobre posibles intrusos o algún programa maligno. Otra medida básica es la protección de nuestro nombre, información personal e imagen; pues, al igual que en la vida fuera del Internet, es necesario verificar con quién y cómo compartimos nuestros datos.

La Ley de Protección de Datos Personales para el Distrito Federal (2014), en su artículo 2, define datos personales como

> La información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

Por lo tanto es recomendable no publicar en redes sociales o páginas poco confiables el domicilio particular y laboral, o imágenes que los muestren o evidencien; de igual forma con nuestro correo electrónico, es preferible mantenerlo de forma discreta u oculto, o bien, crear diferentes cuentas para diferentes usos: laboral, personal, compras, promociones, redes sociales, u otros usos.

Otras precauciones relacionadas son revisar de forma periódica la privacidad de nuestras cuentas y aplicaciones, evitar la sobreexposición de nuestra información y establecer configuraciones como notificaciones de etiquetas, con el fin de disminuir los riesgos de suplantación o robo de información.

Por otro lado, Internet es un canal de dos vías, por lo que debemos tener presente que algún usuario nos puede dañar, pero nosotros también podemos dañar a otros; por ello es importante hacer publicaciones y emitir opiniones de forma sensata y prudente, evitando juicios o señalamientos mal intencionados, discriminatorios y que contengan un lenguaje éticamente correcto.

Otra herramienta de ayuda es mantener contraseñas seguras y una para cada aplicación; se sugiere que contenga palabras difíciles de adivinar y evitar en estas el uso de fechas importantes. En la red se pueden encontrar administradores de contraseñas muy confiables, que facilitan la tarea de conservación y su actualización. Es conveniente tener la configuración de "verificación de dos pasos"

Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

para el inicio de sesiones, ya que esto bloquea casi por completo el robo de nuestras cuentas e información.

Es recomendable vigilar en manos de quién se encuentran nuestros dispositivos móviles, que el PIN no sea un patrón fácil de descifrar y usar uno distinto para cada dispositivo, esto mantiene nuestra información a salvo.

Asimismo, se recomienda verificar los remitentes de correos electrónicos y mensajería instantánea, o las url[3] y los archivos que descargamos; así como desconfiar de aplicaciones o sitios que nos piden datos personales que solo deben tener las instituciones o dependencias, ya que estas acciones pueden evitar que seamos víctimas de delitos.

En cuanto a una navegación segura, es importante restringir nuestro uso de redes públicas o abiertas y, en caso de requerir su empleo, no abrir aplicaciones bancarias o ingresar datos sensibles mientras estemos conectados a esa red; además, comprobar las configuraciones de seguridad de nuestros dispositivos y de nuestras cuentas de redes sociales, correo y demás servicios; verificar la fuente de donde obtenemos información y evitar la difusión de noticias falsas.

Conductas sancionadas

Al navegar por Internet podemos ser objeto de diversos delitos, por ello, los legisladores trabajan para incorporar los temas específicos sobre delitos cibernéticos. Sin embargo, la tarea legislativa y sancionadora se dificulta por la manera tan acelerada en la que se incrementan el uso y los sistemas de Internet; así como los mecanismos nuevos que se implementan a cada día, aunado a la complejidad de seguir los rastros y a los individuos que cometen los delitos. No obstante, algunas de estas conductas ya se encuentran tipificadas en las diversas leyes federales y locales.

Ejemplo de lo anterior se encuentra en el Código Penal Federal que señala y castiga conductas que pueden encuadrarse en los delitos antes descritos:

> Ataques a las vías de comunicación y violación de correspondencia. Artículo166 Bis. A las personas que por razón de su cargo o empleo en empresas de telecomunicaciones, ilícitamente proporcionen informes acerca de las personas que hagan uso de esos medios de comunicación, se les impondrá pena de tres meses a tres años de prisión y serán destituidos de su cargo.
>
> Violación de correspondencia. Artículo 177. A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa.
>
> Pornografía. Comunicación de Contenido Sexual con Personas Menores de Dieciocho Años de Edad o de Personas que no tienen Capacidad para comprender el Significado del Hecho o de Personas que no tienen la Capacidad para Resistirlo. Artículo 199 Septies. Se impondrá de cuatro a ocho años de prisión y multa de cuatrocientos a mil días multa a quien haciendo uso de medios de radiodifusión, telecomunicaciones, informáticos o cualquier otro medio de transmisión de datos, contacte a una persona menor de dieciocho años de edad, a quien no tenga capacidad de comprender el significado del hecho o a persona

[3]Una URL (Uniform Resource Locator) es la dirección única y específica de cada página o recurso que existe en la *web*. Cada página y recurso van enlazados a una URL, pues de otra manera los navegadores no podrían localizar la información demandada por el usuario.

que no tenga capacidad para resistirlo y le requiera imágenes, audio o video de actividades sexuales explícitas, actos de connotación sexual, o le solicite un encuentro sexual.
Violación a la Intimidad Sexual. Artículo 199 Octies. Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización. Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización. Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.

Fraude. Artículo 386. Comete el delito de fraude el que engañando a uno o aprovechándose del error en que éste se halla se hace ilícitamente de alguna cosa o alcanza un lucro indebido.
El delito de fraude se castigará con las penas siguientes:

I.- Con prisión de 3 días a 6 meses o de 30 a 180 días multa, cuando el valor de lo defraudado no exceda de diez veces el salario;
II.- Con Prisión de 6 meses a 3 años y multa de 10 a 100 veces el salario, cuando el valor de lo defraudado excediera de 10, pero no de 500 veces el salario;
III.- Con prisión de tres a doce años y multa hasta de ciento veinte veces el salario, si el valor de lo defraudado fuere mayor de quinientas veces el salario.

Extorsión. Artículo 390. Al que sin derecho obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro o causando a alguien un perjuicio patrimonial, se le aplicarán de dos a ocho años de prisión y de cuarenta a ciento sesenta días multa. (Código Penal Federal, 2021).

Estas conductas sancionadas se incluyen en el Código Penal Federal y, si fuimos víctimas de ellas, podemos realizar una denuncia con base en este instrumento, no importa si fueron cometidas en línea o fuera de esta.

Sin embargo, se debe observar que en algunos tipos penales (con sus diferentes atenuantes y agravantes) no se logra el enjuiciamiento y dictado de la sentencia respectiva, porque los delincuentes son expertos en ocultar sus rastros e identidad y emplean servidores que se localizan fuera del territorio nacional, o desvían las señales a distintos servidores, por lo que estaríamos frente a la extraterritorialidad o transnacionalidad; hay casos en los que esto no se consigue, aun cuando las autoridades trabajen en colaboración y con apoyo de otros organismos o agencias nacionales e internacionales, para combatir y sancionar dichos escenarios, incluso con la participación de la Organización Internacional de Policía Criminal (INTERPOL). [4]

Conclusión

Se requiere trabajar y avanzar a pasos acelerados en leyes, sistemas, tecnología y personal capacitado para la protección del usuario de Internet, considerando los cambios y adaptándonos al nuevo estilo de vida que nos exigen estas dinámicas. Asimismo, es fundamental educar al ciudadano en la prevención de riesgos y conductas éticas en el uso de dispositivos electrónicos, para generar relaciones sanas entre los usuarios y proveedores de servicios. Además, no todos los delitos son cometidos por personas expertas en sistemas informáticos, también el usuario con conocimientos básicos en estas herramientas puede cometerlos, aprovechando la oportunidad, el desconocimiento, la ingenuidad o la alteración emocional de los otros.

[4]La INTERPOL es una organización intergubernamental que cuenta con 194 países miembros. Ayudando a la policía de estos países a colaborar entre sí para hacer del mundo un lugar más seguro.

VOCES Y SABERES

Voces y Saberes. Año 2 núm. 04 marzo-junio 2022

Referencias

Código Penal Federal [CPF], reformado, *Diario Oficial de la Federación* [DOF], 14 de agosto de 1931 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Codigo_Penal_Federal.pdf

Constitución Política de los Estados Unidos Mexicanos *Diario Oficial de la Federación* [DOF], 5 de febrero de 1917 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/*CPEUM*.pdf

Instituto Nacional de Estadística y Geografía, INEGI. (2021, 22 de junio). En *México hay 84.1 millones de usuarios de internet y 88.2millones de usuarios de teléfonos celulares: ENDUTIH 2020.* [Comunicado de prensa]. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

Instituto Nacional de Estadística y Geografía, INEGI. (2021, 5 de julio). *Módulo sobre ciberacoso 2020.* [Comunicado de prensa]. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EstSociodemo/MOCIBA-2020.pdf

Ley de Ciudadanía Digital de la Ciudad de México, *Gaceta Oficial de la Ciudad de México,* 19 de enero de 2020 (México). https://paot.org.mx/centro/leyes/df/pdf/2020/LEY_CIUD_DIGITAL_CDMX_09_01_2020.pdf

Ley Federal de Protección de Datos Personales para el Distrito Federal [LFPDPDF], reformada, *Gaceta Oficial del Distrito Federal,* 18 de diciembre de 2014 (México). http://www.aldf.gob.mx/archivo-f73bdb295c017416ad640607e8aa1275.pdf

vLex. (2020, 9 enero). Ley de Ciudadanía Digital de la Ciudad de México. vLex. https://vlex.com.mx/vid/decreto-abrogan-ley-firma-835441525?from_fbt=1&forw=go&utm_source=addon&fbt=webapp_preview

Organización Mundial de la Salud (OMS). (2020, 27 de abril). *Línea de tiempo COVID-19. OMS.* https://www.who.int/es/news/item/27-04-2020-who-timeline---covid-19

Quesada, A. (2013). Aprendizaje colaborativo en entornos virtuales: los recursos de la Web 2.0. *ERevista de Lenguas Modernas (18),* 337-350.

rtve (2021, 10 de abril). *rtve noticias.* https://www.rtve.es/noticias/20210410/mapa-mundial-del-coronavirus/1998143.shtml

The Seattle Times (2022). Phishing & Pharming. [From Oxford Dictionary]. https://www.seattletimes.com/nation-world/oxford-dictionary-accepts-phishing/#:~:text=Oxford%20Dictionaries%20uses%20databases%20of,programs%20and%20Internet%20chat%20rooms.&text=The%20dictionary%20defines%20phishing%20as,revealing%20their%20credit%2Dcard%20details

Otras lecturas recomendadas

Ang, L., Dubelaar, C., & Lee, B-Ch. (2001, 25-26 June). *To Trust or Not to Trust? A Model of Internet Trust from the Customer's Point of View* [Congress session]. 14th Bled Electronic Commerce Conference. Slovenia. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1090&context=bled2001

Bayer, U. (2005). *TTAnalyze: A Tool for Analyzing Malware.* [Master's Thesis, Technical University of Vienna]. Technical University of Vienna Digital Archive. https://repositum.tuwien.at/bitstream/20.500.12708/12822/2/Bayer%20Ulrich%20-%202005%20-%20TTAnalyze%20a%20tool%20for%20analyzing%20malware.pdf

Glosario de Ciberseguridad. (s.f.). https://www.ssc.cdmx.gob.mx/storage/app/media/Subsecretaria%20de%20Inteligencia%20e%20investigacion%20Policial/Policia%20Cibernetica/Documentos/Descargas/Glosario%20de%20Ciberseguridad.pdf

Palomar de Miguel, J. (2000). *Diccionario para juristas.* Porrúa.